

AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT			1. CONTRACT ID CODE	PAGE 1 OF 9 PAGES
2. AMENDMENT/MODIFICATION NO. 0001		3. EFFECTIVE DATE 09/14/2006	4. REQUISITION/PURCHASE REQ. NO.	5. PROJECT NO. (If applicable)
6. ISSUED BY FEDERAL COMMUNICATIONS COMMISSION 445 12th Street, SW Washington, DC 20554		7. ADMINISTERED BY (If other than Item 6) CODE		
8. NAME AND ADDRESS OF CONTRACTOR (No., street, county, State and ZIP Code) ALL GSA FABS SCHEDULE 520 & IT SCHEDULE 70 FEDERAL SUPPLY SCHEDULE OFFERORS		(X) X	9A. AMENDMENT OF SOLICITATION NO. RFQ06000030	
			9B. DATED (SEE ITEM 11) 09/11/06	
			10A. MODIFICATION OF CONTRACT/ORDER NO.	
			10B. DATED (SEE ITEM 11)	
CODE		FACILITY CODE		

11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS

- ☒ The above numbered solicitation is amended as set forth in Item 14. The hour and date specified for receipt of Offers ☐ is extended, ☐ is not extended.
- Offers must acknowledge receipt of this amendment prior to the hour and date specified in the solicitation or as amended, by one of the following methods:
- (a) By completing items 8 and 15, and returning 1 copies of the amendment; (b) By acknowledging receipt of this amendment on each copy of the offer submitted; or (c) By separate letter or telegram which includes a reference to the solicitation and amendment numbers. FAILURE OF YOUR ACKNOWLEDGMENT TO BE RECEIVED AT THE PLACE DESIGNATED FOR THE RECEIPT OF OFFERS PRIOR TO THE HOUR AND DATE SPECIFIED MAY RESULT IN REJECTION OF YOUR OFFER. If by virtue of this amendment your desire to change an offer already submitted, such change may be made by telegram or letter, provided each telegram or letter makes reference to the solicitation and this amendment, and is received prior to the opening hour and date specified.

12. ACCOUNTING AND APPROPRIATION DATA (If required)

N/A

13. THIS ITEM ONLY APPLIES TO MODIFICATION OF CONTRACTS/ORDERS. IT MODIFIES THE CONTRACT/ORDER NO. AS DESCRIBED IN ITEM 14.

CHECK ONE	A. THIS CHANGE ORDER IS ISSUED PURSUANT TO: (Specify authority) THE CHANGES SET FORTH IN ITEM 14 ARE MADE IN THE CONTRACT ORDER NO. IN ITEM 10A.
	B. THE ABOVE NUMBERED CONTRACT/ORDER IS MODIFIED TO REFLECT THE ADMINISTRATIVE CHANGES (such as changes in paying office, appropriation date, etc.) SET FORTH IN ITEM 14, PURSUANT TO THE AUTHORITY OF FAR 43.103(b).
	C. THIS SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO AUTHORITY OF:
	D. OTHER (Specify type of modification and authority)

E. IMPORTANT: Contractor ☐ is not, ☐ is required to sign this document and return _____ copies to the issuing office.

14. DESCRIPTION OF AMENDMENT/MODIFICATION (Organized by UCF section headings, including solicitation/contract subject matter where feasible.)
This Amendment serves to address questions received. This Amendment also extends the proposal due date to September 18, 2006 at 2:00 pm EST. Accordingly, see following pages.

Except as provided herein, all terms and conditions of the document referenced in Item 9A or 10A, as heretofore changed, remains unchanged and in full force and effect.

15A. NAME AND TITLE OF SIGNER (Type or print)		16A. NAME AND TITLE OF CONTRACTING OFFICER (Type or print)	
		Anthony S. Wimbush, Contracting Officer	
15B. CONTRACTOR/OFFEROR	15C. DATE SIGNED	16B. UNITED STATES OF AMERICA	16C. DATE SIGNED
(Signature of person authorized to sign)		<i>Anthony S. Wimbush</i> (Signature of Contracting Officer)	09/14/06

**QUESTIONS AND ANSWERS (Q&A'S) TO RFQ06000030 FOR
FCC'S "FINANCIAL MANAGEMENT SYSTEMS SUPPORT
SERVICES"**

The following is a compilation of questions received in response to RFQ06000030 and the Government's responses. The questions and comments are listed in the order they were received and appear as they were received. In the event of an inconsistency between these responses and the RFQ, the RFQ shall govern.

Q1. "... is currently reviewing the solicitation documents for the above mentioned opportunity and would like to know if the FCC would consider an extension on the proposal due date? Please advise."

A1. The proposal due date and time is hereby extended through Monday, September 18, 2006 at 2:00 pm, EST.

Q2a. "We respectfully request an **extension** for this solicitation of one week..."

A2a. See A1.

Q2b. "...and also request that you clarify the following note regarding Conflict of Interest that was included in the Instructions:

SPECIAL NOTE: The selected successful offeror will be excluded from competing for a subsequent related requirement for hosting, implementation, migration, and integration services.

The SOW has a COI clause which doesn't address this issue. In addition, it has been the practice of other Federal Agency Procurements for this function that the winning vendor is allowed to perform the follow-on work. Generally the vendors that are conflicted out are those that are currently owners of the software or firms that already perform this work as a Center of Excellence or are service providers for hosting and operations. We are neither.

Please clarify the Conflict of Interest clause."

A2b. The Conflict of Interest Clause is a standard clause that the FCC utilizes in its solicitations and contracts as applicable. As such, it does not specifically address the "special notice" concern.

For the purposes of the instant requirement, the FCC has determined that significant conflict of interest concerns related to program management and program oversight would occur if the successful offeror was also successful in competing for the subsequent work. As such, the FCC's "Special Notice" requirement stands. The successful offeror will be excluded from competing for a subsequent related requirement for hosting, implementation, migration, and integration services.

Q3. "On page 4 of the RFQ Instruction Letter we find 'The price quote shall be submitted as a **Fixed Price Labor Hour/Time and Material quote**'. On page 6 of the SOW, the pricing format includes the line '**Total Fixed Price**'.

Would you please clarify that the task is to be a Time and Materials type, with fixed Labor Hour rates, and how the "Total Fixed Price" item is to be presented in our pricing schedule?"

A3. Yes, the tasks will be of a Time & Materials type with fixed labor hour rates. Your respective pricing shall reflect a "Total Estimated Price".

Q4. "There is reference to a BPA beginning on page 10 of the SOW. Can you clarify, please, that the award vehicle will be a GSA Task Order, not a BPA?"

A4. Yes, the award vehicle will be a GSA Task Order. All references to BPA are hereby deleted for the Clause and the Clause has been updated to reflect the changes. Replace the Clause in its entirety with the attached Clause (see Attachment 1).

Q5. "SOW Section 4.0 (Tasks), Task 3 – Review and Analysis

Question – Please clarify whether the FCC is anticipating a single or many deliverables/reports associated with this task consisting of the review and analysis of the FCC's project management plan and milestones, objectives, and technical and management considerations for initiating and conducting the integration of the new core accounting system."

A5. The FCC anticipates multiple deliverables/reports. As such, the Task has been updated to add the following language;

"As required, the contractor shall provide written and/or oral reports to the COTR."

This language is added as the last sentence of the Task following Subtask 3(s). Please pen & ink in changes.

Q5. "SOW Section 4.0 (Tasks), Task 3 – Review and Analysis

Question – Please clarify the anticipated due date for the deliverable(s) associated with this task."

A5. Due date is "as required". See A5.

Q6. "SOW Section 5 (Pricing Schedule – Compensation)

Question – Please clarify the anticipated contract type. The Price Quote Instructions (RFQ, page 4 of 5) indicate T&M; however, the sample structure under SOW Section 5, appears to suggest FFP. "

A6. See A3.

Q7. "SOW Section 5 (Pricing Schedule – Compensation)

Question – Please clarify how the information requested in Section 5 be provided for the option years where there is no statement of work on which to base a level of effort. Should the offeror just list Labor Category and Rate/Hour for the option years? "

A7. The Statement of Work is the same for the Base Period and Option Periods. The offeror shall submit the estimated # of Hours, the fixed Rate/Hour, and the Total Estimated Price for the Base and each Option Period.

Q8. "SOW Section 7 (Period of Performance)

Question – The Base Period is indicated as September 30, 2006 to September 29, 2007. Option Period 1 is indicated as September 30, 2008 to September 29, 2009. Please clarify whether there should be an intervening option year covering the period of September 30, 2007 to September 29, 2008."

A8. There is no intervening option year. The Period of Performance is updated to reflect the following:

7. PERIOD OF PERFORMANCE

The Period of Performance is:

Base Period: September 30, 2006 to September 29, 2007

If exercised:

Option Period 1: September 30, 2007 to September 29, 2008

Option Period 2: September 30, 2008 to September 29, 2009

Q9. "SOW Section 14.A.4 (Confidentiality)

Question – The solicitation requires an "ongoing" obligation on Contractor personnel with respect to disclosure of information. However, Sections 14.B.1.c and 14.B.1.c appear to impose 6-month and 3-month confidentiality obligations, respectively, for that same information, following expiration of the BPA term. Please clarify the duration of the Contractor's confidentiality obligations under the resultant contract. "

A9. The 6-month reference applies to vendor and vendor personnel involvement in services to any third party (*i.e.*, any party other than the FCC or the Vendor) with respect to any matter that **directly** relates to the subject matter of any tasks under this order. The 3-month reference applies to vendor and vendor personnel involvement in services to any third party (*i.e.*, any party other than the FCC or the Vendor) with respect to any matter that **indirectly** relates to the subject matter of any tasks under this order.

Q10. "SOW Section 16 (Suitability and Security Processing)

Question – What level of security is required of the Contractor Personnel assigned to this effort i.e; low, moderate, high?"

A 10. Moderate

Q11. "RFQ Due Date (3:30pm Eastern Tim, Friday, September 15, 2006)

Question – We formally request that FCC consider granting an extension of the due date for responses. "

A11. See A1.

Attachment 1

14. CONFIDENTIALITY AND CONFLICT OF INTEREST

The following Confidentiality and Conflict of Interest clauses shall be incorporated into the order awarded under this procurement:

A. CONFIDENTIALITY

1. The Vendor and any personnel assigned to work on issued under this order, including any employees, subcontractors, subcontractor employees, consultants, agents, or other representatives of the Vendor (collectively “the contract personnel”) are restricted as to their use or disclosure of non-public information obtained during the period of performance of this order. Non-public information means any information that is not routinely available for public inspection. Section 0.457 of the FCC’s rules (47 C.F.R. § 0.457) lists different types of non-public information maintained at the FCC including, but not limited to, information that is subject to the attorney-client privilege, the attorney work product doctrine, the deliberative process privilege, or any other relevant claims of privilege and exempt from disclosure under the Freedom of Information Act. It is the responsibility of the Vendor and contract personnel to preserve all non-public information in confidence.
2. The Vendor and contract personnel may not discuss or disclose non-public information, either within or outside of the Vendor’s organization, except (a) FCC employees authorized by the Contracting Officer to receive such information; (b) for approved contract personnel who have executed a Non-Disclosure Agreement (Attachment 1 to the RFQ) as necessary for performance of work under this order; or (c) as directed in writing by the Contracting Officer. The Vendor is responsible for ensuring that all contract personnel execute the attached Non-Disclosure Agreement and providing executed Non-Disclosure Agreements to the Contracting Officer before contract personnel commence any work under this order. These procedures apply to any contract personnel assigned to perform work under this order following award.
3. Requests for the use of any non-public information obtained during, or resulting from, the performance of the order must be addressed in writing to, and approved in writing by, the Contracting Officer. In the event the Vendor is issued a subpoena, court order, or similar request seeking information related to this contract, the Vendor will notify the Contracting Officer in writing within one calendar day of knowledge or receipt of such request, whichever is sooner.
4. The prohibition on disclosure of information described above is an ongoing obligation of the Vendor and contract personnel and does not terminate with completion of work under this order or, with respect to contract personnel, upon conclusion of an individual’s employee/consultant/representative relationship

with the Vendor or its subcontractor(s).

B. CONFLICT OF INTEREST

1. The Vendor is expected to provide high quality service to the Commission that is free from bias, and personal and organizational conflicts of interest (*see e.g.*, FAR Part 9.5), including the appearance of impropriety or unprofessional conduct. At all times, the Vendor must exercise organizational independence to ensure its ability to objectively and critically assess the FCC's programs and activities.
 - a. Neither the Vendor nor any contract personnel may perform services under this order that directly relate to matters on which it has worked in the past (other than for the FCC) without explicit authorization in writing from the Contracting Officer. For example, the Vendor may not perform audit work under an order if it, or any contract personnel, had any role or involvement in the preparation, analysis, or review of the work that is being audited. Any such past role or involvement is deemed to create, at a minimum, a potential conflict of interest and must be reported in writing immediately to the Contracting Officer for review and disposition.
 - b. During and after the order term, neither the Vendor nor any contract personnel may dispute the validity of any work product generated under this order in any matter adverse to the interests of the FCC. For example, neither the Vendor nor contract personnel may challenge audit methodologies, findings, etc. on behalf of any entity audited in connection with this order if the Vendor or contract personnel had any role or involvement in the preparation, analysis, or review of such work for the FCC.
 - c. During the order term and for a period of six (6) months thereafter (*i.e.*, 6 months after completion of the task order ordering period or completion of all work performed under any task order task order, whichever is later), neither the Vendor nor any contract personnel may provide services to any third party (*i.e.*, any party other than the FCC or the Vendor) with respect to any matter that directly relates to the subject matter of any tasks under this order. Any such representation is deemed to create, at a minimum, a potential conflict of interest and must be reported in writing immediately to the Contracting Officer for review and disposition.
 - d. During the order term, and for a period of three (3) months after expiration of the order term, neither the Vendor nor any contract personnel may provide services to any third party with respect to any matter indirectly relating to the subject matter of any task under this order without first providing a detailed written explanation of the proposed services to be rendered and obtaining the written consent of the Contracting Officer in connection therewith. The Contracting Officer's consent shall not be unreasonably withheld.
 - e. In connection with both the Vendor's confidentiality obligations in Paragraph A

("Confidentiality") above and the conflict of interest requirements herein, the Vendor must submit, within 7 days of award, a detailed plan and description of its record retention and access practices and its so-called "Chinese Wall" procedures; *e.g.*, procedures for handling and protecting confidential information; procedures for determining the existence of an actual or potential conflict of interest with respect to the Vendor or contract personnel; and controls for limiting and/or monitoring information exchange by contract personnel that would be employed in the event an actual or potential conflict of interest is identified.

2. Offerors shall submit the following information to the Contracting Officer with their responses to this RFQ:
 - a. Name, address, and telephone number of any client of the offeror or any proposed subcontractor(s) or consultant(s), and a description of the services rendered, if, in the two (2) years preceding the date of this solicitation, services were rendered to such client relating directly or indirectly to the subject matter of the services to be provided to the FCC under the instant procurement.
 - b. A description of any policy or advocacy activities by the offeror or any proposed subcontractor(s) or consultant(s) with respect to the FCC or any other Government agency that relate directly or indirectly to the financial management and performance services that are within the scope of the order; *e.g.*, *ex parte* presentations; comments submitted in an agency proceeding; etc.

Any failure to avoid, neutralize, or mitigate any actual or potential conflict, or the appearance of such, to the satisfaction of the Government may render an offeror ineligible for award.

3. The Vendor shall promptly report to the Contracting Officer any changes to the list provided in paragraph 2 above that may arise during the order term. The FCC may also require the Vendor to submit a revised list in its response to a solicitation for any task under this order.
4. The Vendor is required to take all reasonable measures to monitor the existence of actual or potential conflicts of interest, or the appearance of such, during the order term. If the Vendor discovers an actual or potential conflict of interest, or the appearance of such, at any time during the order term, it shall make an immediate and full disclosure in writing to the Contracting Officer of the nature of the conflict (in sufficient detail so that the FCC can determine the existence and extent of the conflict) and the action which the Vendor has taken or proposes to take to avoid, neutralize, or mitigate the conflict.
5. The Contracting Officer may direct the Vendor to avoid, neutralize, or mitigate any actual or potential conflict of interest, or the appearance of such, and may specify particular measures that the Vendor is required to take. The Vendor recognizes that the failure to avoid, neutralize, or mitigate any actual or potential conflict of interest, or the appearance of such, to the satisfaction of the FCC may render it ineligible for

consideration for, or award of, future orders, and/or subject to default termination of any or all orders awarded to the Vendor . If the Vendor fails to disclose an actual or potential conflict of interest, or the appearance of such, of which it is aware, or misrepresents relevant information regarding same to the Contracting Officer, the FCC may take any of the actions described in the preceding sentence and report the Vendor's action to the GSA Contracting Officer for the Vendor's Schedule contract.



**Federal Communications Commission
Washington, DC 20554**

Reply to Attn of: **C&PC**

09/11/06

TO: Interested GSA Financial and Business Solutions (FABS) Schedule 520 And Information Technology (IT) Schedule 70 Firms

SUBJECT: Request for Proposal (RFP) Number RFQ06000030 for the Federal Communications Commission's (FCC) Financial Management Systems Support

The Federal Communication Commission (FCC) is issuing this competitive RFQ to solicit GSA FABS and IT Schedule contract holders for the purpose of entering into a Task Order under the schedule contract. The FCC will conduct this acquisition using Subpart 8.4 under the Federal Acquisition Regulation. If you are interested in this acquisition, you may participate by submitting your response in accordance with the following instructions. Submission shall be via email.

This solicitation will be posted on the FCC website at:
www.fcc.gov/omd/contracts/preaward/. It is the responsibility of each interested vendor to monitor this website for any updates and amendments.

Offerors are required to immediately notify Tony Wimbush via email of their intent to bid. Offerors are required to submit both a written technical quote and a price quote for the purposes of assuring that the prospective Contractor is fully cognizant of the scope of this contract and has the capability to complete all Statement of Work (SOW) requirements.

Offerors are to provide a total solution using the GSA FABS and/or IT Schedules. Offerors may propose appropriate labor categories from their own Schedule contract(s) or Offerors may team with another Schedule holder(s) to offer a blended solution.

All offerors shall certify in writing that their proposed solution falls within the scope of their referenced GSA Schedule contract(s).

If you have questions regarding this requirement, please submit your inquiries immediately via email but **no later than Wednesday, September 13, 2006, 3:00 pm** **Time to Tony Wimbush** at: anthony.wimbush@fcc.gov .

Please be advised that the Government reserves the right to transmit/post those questions and answers of a common interest to all prospective Offerors.

Award will be based upon overall best value to the Government.

All potential offerors are cautioned to strictly adhere to the provisions of their GSA Schedules contract and this RFQ regarding conflicts of interest. Any such matters must be brought to the attention of the Contracting Officer at or before the time offers are due. Please be advised that if an actual or potential personal or organizational conflict exists between your firm and the FCC that cannot be resolved, avoided, or mitigated to the satisfaction of the FCC, then your firm shall not be considered eligible for an award.

All offerors shall follow the following proposal instructions and submit their proposal with the completed proposal cover sheet (copy enclosed). Your **proposal** shall indicate an **acceptance period of no-less-than 60 days** from the due date for submission.

The **proposal shall not exceed 5 pages**, excluding resumes, past performance information, and price information. A page is defined as one side of an 8½" x 11" sheet of white, un-textured paper, single-spaced, with at least one inch margins on all sides, using not smaller than 12 characters per linear inch or be smaller than twelve (12) point, and shall not exceed six (6) lines per vertical inch. Information may be submitted on single or double-sided sheets, but shall not exceed this page limitation. The type for all documents submitted (including charts and graphs) shall be black.

The offer shall be provided electronically via email.

SUBMISSION REQUIREMENTS

Your offer **MUST** cite the appropriate Schedule Contract Number in your quote submission along with your tax identification number (**TIN**) and Dun & Bradstreet Number (**DUNS**), North American Industrial Classification System (**NAICS**), Standard Product Code (**SPC**) and other pertinent information found in Enclosure 2, Quotation Cover Page. Please ensure that your firm is CCR Certified (<http://www.ccr.gov>).

ASSUMPTIONS, CONDITIONS, OR EXCEPTIONS

Offerors must acknowledge all (if any) assumptions, conditions, or exceptions with **any** of the terms and conditions of this solicitation including the SOW. If not noted in this section of your quote, it will be assumed that the offeror proposes no assumptions for award, and agrees to comply with all of the terms and conditions as set forth herein.

TECHNICAL QUOTE INSTRUCTIONS

Offerors shall provide a technical quote that includes the following three areas: To facilitate evaluation of proposals offerors are requested to present the narrative portion in the format outlined below:

A. Technical Approach

Quoters are required to provide a written technical proposal that explains their proposed technical approach to meeting the requirements within established timeframes. The discussion should, at a minimum, include:

- An understanding of core financial systems;
- Methodology for performing the required services;
- Proposed mix of personnel;
- Estimated hours;
- A discussion of available COTS for enterprise resource solutions used in the Federal Government; and
- Methodology for migrating to a new system.

B. Staffing

Quoters are required to provide a written technical proposal that explains their proposed staffing and pertinent industry experience that satisfies the requirements defined in this document. Please describe your proposed staffing and industry experience with contracts and organizations of similar size scope and complexity to this requirement. Quoters are to submit the resumes of all proposed staff. Resumes should describe the professional expertise, professional certifications, and academic backgrounds of the staff members who will be assigned to this engagement.

C. Past Performance

Quoters are required to provide a written technical proposal that explains their past performance (at least 3 references) that satisfies the requirements defined in this document.

The Offeror shall identify three (3) contracts/task orders with the Federal Government and/or commercial customers that demonstrate recent and relevant past performance. Recent is defined as within the last three years. Relevant is defined as work similar in complexity and magnitude of the work described in this Statement of Work.

Offerors proposals shall include the following information:

- Project title;
- Description of the project;
- Contract number;
- Contract amount;
- Government Agency/Organization;
- COTR's name, address, and phone number;
- Contracting Officer's name, address, and phone number;
- Contract and, if applicable, task order number;
- Current status, e.g., completed and/or if in progress, start and estimated completion dates;
- Dollar value and type of contract;
- Name of company being referenced;
- SOW paragraphs that the reference applies to;

- Key personnel (please highlight those individuals who worked on the relevant project(s) and are also being proposed for this effort.); and
- A brief narrative of why you deem the reference to be relevant to this effort

The Government may also consider information obtained through other sources. Past performance information will be utilized to determine the quality of the contractor's past performance as it relates to the probability of success of the required effort.

Technical proposals that merely parrot the requirements set forth in the SOW and state that the "Offeror will perform the statement of work" or similar verbiage will be considered non-responsive and will not receive further consideration. The FCC is interested only in proposals that demonstrate the Offeror's requisite expertise in performing engagements of this type as illustrated by the Offeror's description of how it proposes to perform the requirements set forth in the Statement of Work (SOW).

***Note:** The Offeror shall ensure that personnel proposed are current in the knowledge required to support the tasking. The personnel proposed must be available and assigned to the project.*

PRICE QUOTE INSTRUCTIONS

Your price quote shall be a separate volume from your technical quote. The price quote shall be submitted as a **Fixed Price Labor Hour/Time and Material quote** and shall be based on your current GSA Schedule contract's fully burdened labor rates for all applicable labor categories, utilizing any and all discounts.

- (1) Identify the labor category(s) to be utilized for this effort, a description of the skills and experience per category, and the number of hours and hourly rate(s) proposed, and any other proposed associated costs, for calculating the proposed price .
- (2) Provide a copy of the Offeror's GSA Contract (including contract clauses) listing the applicable labor categories and fixed rates. Fixed rates shall include all costs and fees, including overhead and profits, and shall identify any reduction in schedule rates offered.
Offerors are encouraged to discount their labor rates.

EVALUATION & BASIS FOR AWARD

This procurement shall be conducted giving each solicited firm a fair opportunity by selecting a quote based on the best combination of price and qualitative merit and reduce the administrative burden of all parties. Fair opportunity is based on the premise that, if all offers are of approximately equal qualitative merit, award will be made to the Offeror with the lowest overall evaluated price. However, the Government will consider awarding to an Offeror with higher qualitative merit if the Contracting Officer determines it to be in the Government's best interest.

The Statement of Work serves as the Government's baseline requirements. All offers will be judged against these requirements. Price and technical merit will be considered equal in importance and will not be assigned weights. **The Government intends to award without discussions.**

Please note that this request does not commit the Government to pay any costs incurred in the submission of your offer, nor to contract for said services. Note also, that full, accurate, and complete information is required by this request in accordance with 18 U.S.C. § 1001 which also prescribes the penalties for making false statements.

SPECIAL NOTE: The selected successful offeror will be excluded from competing for a subsequent related requirement for hosting, implementation, migration, and integration services.

Offers shall be emailed to anthony.wimbush@fcc.gov .

The RFQ due date (closing date) is 3:30pm Eastern Time, Friday, September 15, 2006.

Inquiries regarding this procurement may be addressed to the undersigned by telephone call on 202-418-0932 or by email at anthony.wimbush@fcc.gov .

Anthony S. Wimbush
Contracting Officer

Enclosures:

1. Statement of Work
2. Proposal Submittal Cover Sheet

**FCC FINANCIAL MANAGEMENT SYSTEMS SUPPORT
STATEMENT OF WORK**

TABLE OF CONTENTS

1.0	INTRODUCTION	2
2.0	OBJECTIVE	2
3.0	SCOPE OF WORK	2
4.0	TASKS	3
5.0	DELIVERABLES	6

1.0 INTRODUCTION

The FCC plans to implement a new financial management system, following emerging Federal guidelines associated with the Financial Management Line of Business (FMLoB) initiative, using Commercial Off-the-Shelf (COTS) software packages hosted at an approved Shared Service Center. During FY 2007, the FCC plans to solicit bids to migrate the agency from the Federal Financial System (FFS) hosted by the Department of Interior's (DOI) National Business Center to a new core financial system and to host the proposed consolidated core financial management system at one of the approved Shared Service Centers. In FY 2008 the FCC will begin its migration to the replacement system and will begin to consolidate key financial management functions (such as general ledger, accounts payable, accounts receivable, budget formulation and execution) into the new core financial system. The agency plans to complete the migration of its core accounting system by October 2009 (one year in advance of DOI published deadline for discontinuing support for FFS.)

The Associate Managing Director – Financial Operations (AMD-FO) needs Contractor support for comprehensive project planning, coordination, and management of this effort. The Contractor shall be required to analyze and document financial management business processes, as well as financial management systems and electronic interfaces. The Contractor must have expert knowledge about project management as well as the hardware and software used to facilitate control, monitoring and reporting of an agency's fiscal resources, including "mixed financial systems" also used for non-financial management purposes.

2.0 OBJECTIVE

The objective of this procurement action is to obtain financial management systems expertise for initiation, planning, development, integration and eventual migration to a new core accounting system. The Contractor shall have experience with Federal core financial management system requirements and best practices, relevant Commercial-Off-The-Shelf (COTS) products and enterprise resource planning (ERP) tools, consolidated financial systems design, development, information technology (IT) interfaces, integration and hosting activities. The Contractor shall provide technical expertise in all areas of core financial system project management, system lifecycle development, system requirements, design, migration planning, installation and implementation as well business process reengineering. The Contractor shall be considered a member of the Core Financial Systems Replacement Project Team.

3.0 SCOPE OF WORK

The Contractor shall provide qualified Project Management Specialists, Systems Analysts and/or Systems Accounts by degree or training, with expertise in federal rules, regulations, and legislation governing financial management and systems accounting as well as knowledge and experience in the design and implementation of financial accounting systems. The proposed personnel shall have financial systems background and financial systems implementation experience. The proposed personnel must be thoroughly familiar with Office of Management and Budget (OMB) guidance and directives on financial management, project management, earned value management systems and other relevant topics. Proposed personnel must have experience compiling system development life cycle (SDLC) documentation, evaluating financial

management and accounting requirements and data information/technology initiatives, coordinating data conversions, evaluating business processes for automation purposes, responding to Federal Information Security Management Act (FISMA) related security assessments, and reviewing user documentation and training materials for financial systems.

4.0 TASKS

The Contractor shall provide review and analyses support of the FCC's project management objectives and approach for initiation, development, and integration of a new core accounting system. The Contractor shall complete each of the tasks identified below and provide deliverable items to the COTR.

Task 1 – Project Initiation

The Contractor shall assist the FCC initiate the migration to a new core financial system. This support shall include, but not be limited to, the Contractor developing and maintaining the FCC's preliminary project management plans and milestones for migration to a new consolidated financial management and accounting system. The Contractor shall consider relevant Federal migration planning guidance provided by the General Services Administration (GSA) Financial Systems Integration Office regarding the Financial Management Line of Business (FMLoB) initiative (www.fsio.gov/fsio/fsiodata/fsio_fmlob.shtml).

The Contractor shall develop, with input from the FCC's designated project team, project related products including, but not limited to:

1. Project goals, governance structure, and overall approach.
 2. Project Management Plan and materials dealing with key activities, deliverables, dependencies, timelines, constraints, and assumptions.
 3. Project Resource Plan and supporting materials identifying funding, personnel, and other resources needed.
 4. Project Risk Mitigation Plan.
 5. Project Change Management and Communications Plan.
 6. FCC's System Development Lifecycle (SDLC) deliverables.
 7. Acquisition Plan and solicitation materials.
 8. Migration/Transition Plan and materials that address pre-implementation coordination, user documentation, training, implementation planning, etc.
 9. Project Independent Verification and Validation (IV&V) Audit Plan.
- b) Deliverables: These deliverables shall be provided to the COTR no later than thirty (30) work days after award of the contract for review by the FCC. All FCC comments shall be incorporated into the final report no later than forty five (45) work days after award of the contract.

Task 2 – Business Process Modeling

The Contractor shall examine existing FCC financial management processes and develop an “As Is” document. This document shall identify each of the processes used by the FCC to accomplish its financial management operations and identify inefficiencies in the current processes as well as identify effective processes. The document should also propose solutions to the inefficient processes that best fit with COTS. The Contractor shall provide a draft report to be reviewed by the Core Financial System Team no later than seventy-five (75) work days after award of the contract. The Contractor shall incorporate the Team’s comments into the final “As is” document no later than ninety (90) work days after award of the contract.

Task 3 – Review and Analysis

The Contractor shall conduct a complete and thorough review and analysis of the FCC's project management plan and milestones, objectives, and technical and management considerations for initiating and conducting the integration of the new core accounting system. This review and analysis shall include, but not be limited to, steps 2.2 through 9.7 as identified in FMLoB guidelines and the project management objectives and approach for:

- a) System Architecture Concept. Does the proposed system architecture concept meets the project’s objectives, use COTS, is interoperable with FCC systems, is compliant with industry standards, is compliant with the Enterprise Architecture, is scaleable, and provides the interfaces needed to exchange data with internal and external entities.
- b) System Sufficiency. Identify the degree to which all project objectives, considerations, and constraints are met or addressed for the functional areas assessment and, where necessary, identify weaknesses and propose solutions.
- c) Scalability. Will the design be scalable to support increases in users, data increases, and mandated changes when identified.
- d) Databases. Identify the locations and purposes of proposed databases and the methods to synchronize and interface databases.
- e) Security and Privacy Compliance. Does the proposed solution meet all Government Information Security Reform Act (GISRA) and/or FCC security and privacy requirements.
- f) Federal Financial Management Improvement Act (FFMIA) Compliance. Does the proposed solution comply with all FFMIA, Federal Accounting Standards Advisory Board (FASAB), and OMB Form and Content requirements.
- g) Software Process and Gap Analysis. Has the proposed solution been fully compared to what exists and is needed; how gaps will be identified; and how will the proposed solution resolve the gaps.
- h) Business Processes. Evaluate the FCC’s business processes for automation purposes and, where necessary, identify weaknesses and propose solutions.
- i) Back up and Recovery. Has the proposed solution fully addressed back up and recovery to ensure continuity of operations.
- j) Documentation. Review existing financial accounting systems documentation and, where

necessary, identify weaknesses and propose solutions.

- k) Procedures. Review existing procedures, reports and proposals related to financial accounting systems and, where necessary, identify weaknesses and propose solutions.
- l) SDLC Documentation. Review existing SDLC documentation and, where necessary, identify weaknesses and propose solutions.
- m) GISRA Assessments. Evaluate the FCC's GISRA self assessments and, where necessary, identify weaknesses and propose solutions.
- n) User Documentation and Training Material. Review the FCC's User documentation and training materials requirements for the core financial system and, where necessary, identify weaknesses and propose solutions.
- o) Data Conversion Procedures. Review data conversions procedures and, where necessary, identify weaknesses and propose solutions.
- p) Data Warehouse Requirements. Review the data warehouse requirements and, where necessary, identify weaknesses and propose solutions.
- q) Implementation Activities. Review the implementation team activities and, where necessary, identify weaknesses and propose solutions.
- r) System Testing. Review the FCC's system testing plan activities and, where necessary, identify weaknesses and propose solutions.
- s) Hosting. Review the FCC's hosting requirements and, where necessary, identify weaknesses and propose solutions.

Task 4 - Monthly Status Report

The Contractor shall submit a monthly status report for work done from the first day through the last calendar day of the previous month. The status report shall describe the progress achieved during the past month, plans for the forthcoming month, any problems incurred and resolution, any anticipated or required FCC action, and a detailed breakdown of the total hours performed on the task. The report shall include an explanation of cost, performance and schedule for the preceding month. These reports shall provide the COTR sufficient information in order to validate and certify the Contractor's performance for that time period.

The Contractor shall provide the monthly status report to the COTR no later than the 5th day of the following month for review by the FCC.

Task 5 - Weekly Status Meetings

The Contractor shall schedule regular weekly status meetings with the COTR, the Core Financial System Implementation Team, and other FCC staff as required. The schedule for weekly status meeting shall be established at the project kick-off meeting. The purpose of the meeting is to maintain an exchange of technical information, discuss and report on tasks accomplished during the preceding week and tasks scheduled to be accomplished in the upcoming week, address any

outstanding issues that impact the progress, timeline or costs of the project, and identify any problems encountered which require FCC action. The Contractor shall prepare an agenda for each meeting and, within 1 working day after each meeting, provide meeting minutes and action items to all participants at these meetings. The agenda and minutes of these weekly meetings shall be provided to the COTR and the Core Financial System Implementation Team in an electronic and printed format.

The Contractor shall make all necessary arrangements to schedule meeting facilities and audio-visual equipment (if required), notify meeting participants, and prepare the meeting agenda for the weekly meetings.

5.0 DELIVERABLES

The Contractor shall complete the tasks identified above and provide deliverable items to the COTR. The COTR shall coordinate the review of each deliverable with the Core Financial System Implementation Team, and other FCC staff as required. The COTR will provide comments to the Contractor within ten (10) working days of the submission of each item. In the case of document deliverables the Contractor shall incorporate FCC comments and return a revised final deliverable document to the COTR within five (5) working days of receipt. All deliverables shall become the property of the FCC. Each document deliverable shall be submitted in three (3) hard copies and in an acceptable electronic format, using Microsoft Excel, Microsoft Word, Microsoft Project, or any other format that is mutually agreed upon by the COTR and the Contractor. The time frames and format requirements apply to all written reports and documents to be delivered to the FCC. Appropriate charts or graphics shall support all written deliverables, including monthly project status reports, weekly meetings, or presentations.

5. PRICING SCHEDULE - COMPENSATION

The price of this effort is subject to the terms and conditions of the referenced contract. The fully burdened labor rates shown below shall be effective for the total duration of the period of performance of this task order:

<u>Labor Category</u>	<u># of Hours</u>	<u>Rate/Hour</u>	<u>Total Amount</u>
------------------------------	--------------------------	-------------------------	----------------------------

Total Fixed Price:

Note: Travel is not anticipated for this

6. AVAILABILITY OF FUNDS

Funds are not presently available for this contract. The Government's obligation under this contract is contingent upon the availability of funds from which payment for contract purposes can be made. No legal liability on the part of the Government for any payment may arise until funds are made available to the Contracting Officer for this contract and until the Contractor receives notice of such availability, to be confirmed in writing by the Contracting Officer. It is anticipated that this order will be incrementally funded.

7. PERIOD OF PERFORMANCE

The Period of Performance is:

Base Period: September 30, 2006 to September 29, 2007

If exercised:

Option Period 1: September 30, 2008 to September 29, 2009

Option Period 2: September 30, 2009 to September 29, 2010

8. PLACE OF PERFORMANCE--SERVICES

The services specified by this contract shall be performed at the following location(s):

FEDERAL COMMUNICATIONS COMMISSION (Primary Services)
445 12th Street, S.W.
Washington, DC 20554

And

Contractor Facilities (As Required)

To be Proposed (TBP)

9. KEY PERSONNEL

A. The Contractor shall identify "key personnel" to be assigned to perform the required work. The key personnel are considered to be essential to the work being performed for Commission.

The following personnel are designated as Key Personnel for purposes of this task order:

<u>Labor Category</u>	<u>Name</u>	<u>Hours</u>
-----------------------	-------------	--------------

To be Proposed (TBP)

B. The Contractor agrees that the above key personnel shall not be removed from the contract effort, replaced or added to the contract without a compelling reason and without compliance with paragraphs (C) and (D) hereof. The Government will not approve substitutions for the sole convenience of the contractor.

C. If any change to the key personnel position becomes necessary (substitutions or additions), the Contractor shall immediately notify the Contracting Officer in writing, accompanied by the resume of the proposed replacement personnel who shall be of at least substantially equal ability and qualifications as the individuals currently approved for that category.

D. No substitution or replacement of the key personnel shall be approved **within the first ninety (90) days** after contract award.

E. All requests for approval of changes hereunder must be in writing, via email, and provide a detailed explanation of circumstances necessitating the proposed change. Request for changes should be made whenever the need is identified. Beside the resume, the request must also provide:

- 1) a comparison and qualifications to those set forth in the accepted resume proposed for substitution;
- 2) a signed employee non-disclosure agreement;
- 3) number of hours the Contractor will provide at his/her own expense to train the proposed replacement; and,
- 4) any other information requested by the Contracting Officer to reach a decision.

The Contracting Officer will evaluate such requests and promptly notify the Contractor of his/her approval or disapproval in writing.

10. DESIGNATION OF CONTRACTING OFFICER'S TECHNICAL REPRESENTATIVE

A. The Contracting Officer's Technical Representative (COTR) is as follows:

COTR: To Be Determined (TBD)

B. The COTR is responsible for the technical direction of the contract work. In no event, however, will any understanding, agreements, modification, change order, or other matter deviating from the terms of this contract be effective or binding upon the Government unless formalized by proper contractual document executed by the Contracting Officer prior to completion of the contract.

C. The Contracting Officer shall be informed as soon as possible of any actions or inactions by the contractor or the Government which may affect the price, required delivery or completion times stated in the contract, so that the contract may be modified if necessary. Whenever, in the opinion of the contractor, the COTR requests efforts outside the scope of the contract, the contractor shall advise the COTR. If the COTR persists and there still exists a disagreement as to proper contractual coverage, the Contracting Officer should be notified immediately, preferably in writing if time permits. Proceeding with work without proper contractual coverage could result in non-payment.

D. A copy of the COTR delegation letter shall be provided as an attachment after award.

11. CONTRACT ADMINISTRATION

The Contracting Officer is the only person authorized to approve changes. This authority remains solely with the Contracting Officer. In the event the Contractor effects any changes at the

direction of any person other than the Contracting Officer, the changes will be considered to have been made without authority and NO adjustment will be made in the contract price to cover any INCREASE incurred as a result thereof.

A. The Contractor point of contact is:

To Be Proposed (TBP)

Phone:

Fax:

B. The Government points of contact are as follows:

1. Procuring Contracting Officer: Wilma S. Mooney

Address: FCC/OMD/AO/CPC
445 12th Street, SW
Room No. 1A524
Washington, DC 20254

Phone: (202) 418-1865

Fax: (202) 418-0237

2. Contract Administrator/Contract Specialist: Anthony S. Wimbush

Address: FCC/OMD/AO/CPC
445 12th Street, SW
Room No. 1A511
Washington, DC 20254

Phone: (202) 418-0932

Fax: (202) 418-0237

3. Contracting Officer's Technical Representative (COTR): To Be Determined

Address:

Phone:

Fax:

12. GOVERNMENT AND CONTRACTOR RELATIONSHIPS

The Commission and the Contractor understand and agree that the services to be provided under this contract by the Contractor to the FCC are non-personal services. The parties recognize that no employee relationship exists or will exist under this contract. The Contractor contracts with the FCC to furnish the specified services fully described herein and is accountable to the FCC only for furnishing such services, materials, or work ordered.

13. ACCEPTANCE —SINGLE LOCATION

The Contracting Officer or authorized representative will accomplish acceptance at the Federal Communications Commission, 445 12th Street S.W, Washington, DC 20554. For the purpose of this clause, the Contracting Officer's Technical Representative named in this task order is the authorized representative. The Contracting Officer reserves the right to unilaterally designate a different FCC agent as the authorized representative. The Vendor will be notified by a written notice or by a copy of the delegation of authority if different representative is designated.

Acceptance shall be deemed to have occurred constructively--for the sole purpose of computing an interest penalty that might be due the Vendor under the Prompt Payment Act--on the 30th day after the Vendor has delivered the supplies or services in accordance with the terms and conditions of the contract. In the event that actual acceptance occurs within the constructive acceptance period, the determination of an interest penalty shall be based on the date of the actual acceptance.

14. CONFIDENTIALITY AND CONFLICT OF INTEREST

The following Confidentiality and Conflict of Interest clauses shall be incorporated into each task order awarded under this procurement and any task orders issued under such BPA(s):

A. CONFIDENTIALITY

1. The Vendor and any personnel assigned to work on any task order issued under this BPA, including any employees, subcontractors, subcontractor employees, consultants, agents, or other representatives of the Vendor (collectively “the contract personnel”) are restricted as to their use or disclosure of non-public information obtained during the ordering period of this task order or the period of performance of any task order(s) issued under this task order (collectively, the “BPA/order term”). Non-public information means any information that is not routinely available for public inspection. Section 0.457 of the FCC’s rules (47 C.F.R. § 0.457) lists different types of non-public information maintained at the FCC including, but not limited to, information that is subject to the attorney-client privilege, the attorney work product doctrine, the deliberative process privilege, or any other relevant claims of privilege and exempt from disclosure under the Freedom of Information Act. It is the responsibility of the Vendor and contract personnel to preserve all non-public information in confidence.
2. The Vendor and contract personnel may not discuss or disclose non-public information, either within or outside of the Vendor’s organization, except (a) FCC employees authorized by the Contracting Officer to receive such information; (b) for approved contract personnel who have executed a Non-Disclosure Agreement (Attachment 1 to the RFQ) as necessary for performance of work under the BPA; or (c) as directed in writing by the Contracting Officer. The Vendor is responsible for ensuring that all contract personnel execute the attached Non-Disclosure Agreement and providing executed Non-Disclosure Agreements to the Contracting Officer before contract personnel commence any work under this BPA. These procedures apply to any contract personnel assigned to perform work under this task order following award.

3. Requests for the use of any non-public information obtained during, or resulting from, the performance of the task order must be addressed in writing to, and approved in writing by, the Contracting Officer. In the event the Vendor is issued a subpoena, court order, or similar request seeking information related to this contract, the Vendor will notify the Contracting Officer in writing within one calendar day of knowledge or receipt of such request, whichever is sooner.
4. The prohibition on disclosure of information described above is an ongoing obligation of the Vendor and contract personnel and does not terminate with completion of work under this task order or, with respect to contract personnel, upon conclusion of an individual's employee/consultant/representative relationship with the Vendor or its subcontractor(s).

B. CONFLICT OF INTEREST

1. The Vendor is expected to provide high quality service to the Commission that is free from bias, and personal and organizational conflicts of interest (*see e.g.*, FAR Part 9.5), including the appearance of impropriety or unprofessional conduct. At all times, the Vendor must exercise organizational independence to ensure its ability to objectively and critically assess the FCC's programs and activities.
 - a. Neither the Vendor nor any contract personnel may perform services under this task order that directly relate to matters on which it has worked in the past (other than for the FCC) without explicit authorization in writing from the Contracting Officer. For example, the Vendor may not perform audit work under a task order if it, or any contract personnel, had any role or involvement in the preparation, analysis, or review of the work that is being audited. Any such past role or involvement is deemed to create, at a minimum, a potential conflict of interest and must be reported in writing immediately to the Contracting Officer for review and disposition.
 - b. During and after the BPA/order term, neither the Vendor nor any contract personnel may dispute the validity of any work product generated under this task order in any matter adverse to the interests of the FCC. For example, neither the Vendor nor contract personnel may challenge audit methodologies, findings, etc. on behalf of any entity audited in connection with this task order if the Vendor or contract personnel had any role or involvement in the preparation, analysis, or review of such work for the FCC.
 - c. During the BPA/order term and for a period of six (6) months thereafter (*i.e.*, 6 months after completion of the task order ordering period or completion of all work performed under any task order task order, whichever is later), neither the Vendor nor any contract personnel may provide services to any third party (*i.e.*, any party other than the FCC or the Vendor) with respect to any matter that directly relates to the subject matter of any task issued under this BPA. Any such representation is deemed to create, at a minimum, a potential conflict of interest and must be reported in writing immediately to the Contracting Officer for review and disposition.
 - d. During the BPA/order term, and for a period of three (3) months after expiration of the BPA/order term, neither the Vendor nor any contract personnel may provide services to

any third party with respect to any matter indirectly relating to the subject matter of any task issued under this task order without first providing a detailed written explanation of the proposed services to be rendered and obtaining the written consent of the Contracting Officer in connection therewith. The Contracting Officer's consent shall not be unreasonably withheld.

- e. In connection with both the Vendor's confidentiality obligations in Paragraph A ("Confidentiality") above and the conflict of interest requirements herein, the Vendor must submit, within 7 days of task order award, a detailed plan and description of its record retention and access practices and its so-called "Chinese Wall" procedures; *e.g.*, procedures for handling and protecting confidential information; procedures for determining the existence of an actual or potential conflict of interest with respect to the Vendor or contract personnel; and controls for limiting and/or monitoring information exchange by contract personnel that would be employed in the event an actual or potential conflict of interest is identified.
2. Offerors shall submit the following information to the Contracting Officer with their responses to this RFQ:
 - a. Name, address, and telephone number of any client of the offeror or any proposed subcontractor(s) or consultant(s), and a description of the services rendered, if, in the two (2) years preceding the date of this solicitation, services were rendered to such client relating directly or indirectly to the subject matter of the services to be provided to the FCC under the instant procurement.
 - b. A description of any policy or advocacy activities by the offeror or any proposed subcontractor(s) or consultant(s) with respect to the FCC or any other Government agency that relate directly or indirectly to the financial management and performance services that are within the scope of the BPA; *e.g.*, *ex parte* presentations; comments submitted in an agency proceeding; etc.

Any failure to avoid, neutralize, or mitigate any actual or potential conflict, or the appearance of such, to the satisfaction of the Government may render an offeror ineligible for award of a task order.

3. The Vendor shall promptly report to the Contracting Officer any changes to the list provided in paragraph 2 above that may arise during the task order term. The FCC may also require the Vendor to submit a revised list in its response to a solicitation for any task under this task order.
4. The Vendor is required to take all reasonable measures to monitor the existence of actual or potential conflicts of interest, or the appearance of such, during the task order term. If the Vendor discovers an actual or potential conflict of interest, or the appearance of such, at any time during the task order term, it shall make an immediate and full disclosure in writing to the Contracting Officer of the nature of the conflict (in sufficient detail so that the FCC can determine the existence and extent of the conflict) and the action which the Vendor has taken or proposes to take to avoid, neutralize, or mitigate the conflict.

5. The Contracting Officer may direct the Vendor to avoid, neutralize, or mitigate any actual or potential conflict of interest, or the appearance of such, and may specify particular measures that the Vendor is required to take. The Vendor recognizes that the failure to avoid, neutralize, or mitigate any actual or potential conflict of interest, or the appearance of such, to the satisfaction of the FCC may render it ineligible for consideration for, or award of, future task orders, and/or subject to default termination of any or all task orders awarded to the Vendor. If the Vendor fails to disclose an actual or potential conflict of interest, or the appearance of such, of which it is aware, or misrepresents relevant information regarding same to the Contracting Officer, the FCC may take any of the actions described in the preceding sentence and report the Vendor's action to the GSA Contracting Officer for the Vendor's Schedule contract.

15. INVOICES

A. Invoices shall be submitted electronically, by task order, **by the 15th of every month to the FCC Travel/ Operations Group, Room #1A761, 445 12th Street, S.W., Washington, DC 20554.** To constitute a proper invoice, the invoice must include the following information and/or attached documentation:

- (1) Name of the business concern, invoice number and invoice date;
- (2) Task order number, or authorization for delivery of property or performance of services;
- (3) Description, price, and quantity of property and services actually delivered or rendered;
- (4) Shipping and payment terms;
- (5) Name (where practicable), title, phone number, and complete mailing address of responsible official to whom payment is to be sent;
- (6) Other substantiating documentation or information as required by the contract; and,
- (7) Receipts to support all out-of-pocket expenses incurred by the Vendor.

B. Submission of invoices:

- (1) Invoices shall be submitted via email to: FO-Einvoices@fcc.gov. **In addition, copies of the emailed invoices shall also be sent to the CO and COTR.** The address is as follows: FCC Travel/ Operations Group, Room #1A761, 445 12th Street, S.W., Washington, DC 20554

The invoice will contain a statement signed by a responsible official of the concern substantially similar if not identical to the following:

I certify that the items above have been delivered in accordance with the contract, and that all charges are true, correct, and have not been previously billed.

Vendor 's Signature

The commission will return all improper invoices without action.

(2) Interest on Overdue Payment

Determination of interest due will be made in accordance with the provisions of the Prompt Payment Act and Office of Management and Budget Circular A-125.

(3) Payment due date:

- (a) Unless otherwise specified in the contract, payments under this task order will be made on the 30th calendar day after the later of

The date of actual receipt of a proper invoice in the office designated to receive the invoice, or

(ii) The date tasks are formally accepted by the Government.

- (b) If the services covered by a submitted invoice are rejected for failure to conform to the technical requirements of this contract, the provisions stated above will (i and ii) apply to the properly resubmitted document.

16. SUITABILITY AND SECURITY PROCESSING

1. General

1.1 All task order personnel are subjected to background investigations for the purpose of suitability determinations. Based on their proposed duties, some task order personnel may also be required to have security clearance determinations. No task order personnel may be assigned to work on the task order without a favorable initial review of the OF 306, *Declaration for Federal Employment* (http://www.opm.gov/forms/pdf_fill/of0306.pdf) or a written waiver from the FCC Security Operations Center (SOC).

1.2 Suitability, waiver, and security clearance determination investigations are currently conducted through the FCC Security Operations Center (202- 418-7884). The individual task order employee will be provided with a review process before a final adverse determination is made. The FCC requires that any task order personnel found not suitable, or

who has a waiver cancelled, or is denied a security clearance, **be removed by the Vendor during the same business day that the determination is made.**

1.3 If the task order personnel is re-assigned and the new position is determined to require a higher level of risk suitability than the task order personnel currently holds, the individual may be assigned to such position while the determination is reached by the SOC. A new A-600 shall be necessary for the new position.

1.4 Task order personnel working as temporary hires (for ninety (90) days or less) must complete and receive a favorable initial review of the OF 306 and complete the task order personnel section of the FCC Form A-600, "FCC Contractor Record Form." If during the term of their employment they will have access to any FCC network application, they must also complete and sign the FCC Form A-200, "FCC Computer System Application Access Form."

2. At Time of Task Order Award

2.1 The FCC Security Operations Center must receive the completed, signed OF 306 for each proposed individual member of the contract personnel (i.e., "contract employee") at the time of task order award. Resumes for all personnel proposed for assignment on the task order should be provided to the Security Office prior to the time of in-take processing (see below, 2.3.2). **The FCC Security Operations Center requires up to five (5) working days (from the date they are received) to process the OF 306 before any employee is allowed to begin work on the contract. A written waiver from the SOC may be obtained in special circumstances.**

All task order personnel, regardless of task description, must complete this form. Without an approved, completed OF 306 on file at the SOC, no Vendor employee may begin work. An approved OF 306 is one that has passed initial review by the SOC. During the course of the SOC review of the OF 306, the task order personnel may be interviewed by SOC staff regarding information on their OF 306.

2.2 In addition, the Vendor is responsible for submission of completed, signed computer security forms for each employee prior to that person beginning work on the TASK ORDER (See Attachment No. 4, FCC Instruction 1479.1, FCC Computer Security Program Directive and sample forms.) These forms should be submitted to the FCC Computer Security Office.

2.3 The COTR shall begin processing their section of the FCC task order Personnel Record (FCC Form A-600) at this time. This form, with the COTR and CO portions completed, will be distributed at the time of task order award and must be submitted to the SOC within ten (10) working days.

2.4 The Office of Personnel Management (OPM) will issue a Certificate of Investigation (CIN) following the appropriate background investigation. The SOC notifies the CO and COTR and task order personnel who have received a favorable adjudication so they may receive their permanent access credential.

3. IDENTITY PROOFING, REGISTRATION AND CHECKOUT REQUIREMENTS

3.1 Locator and Information Services Tracking (LIST) Registration

The Security Operations Center maintains a Locator and Information Services Tracking (LIST) database, containing contact information for all Commission and task order employee personnel, regardless of work location.

The task order employee's FCC Form A-600, "FCC Contractor Record Form" captures the information for data entry into the LIST system.

3.2 Intake Processing

3.2.1 Following the processing of the OF 306 and an initial favorable suitability determination, (unless otherwise waived) the task order personnel shall report to the FCC for identity verification and access badge issuance on their first scheduled workday.

3.2.2 All new task order personnel must be escorted to the SOC by either the CO or COTR responsible for the contract. At this time the Vendor personnel must present two forms of identification; one of which must be a picture ID issued by a state, or the Federal, government. The other piece of identification should be the original of one of the following:

- U.S. Passport (unexpired or expired)
- Certificate of U.S. Citizenship (Form N-560 or N-561)
- Certificate of Naturalization (Form N-550 or N-570)
- School ID
- Voter's registration card
- U.S. Military card
- Military dependent's ID card
- U.S. Coast Guard Merchant Mariner card
- Native American Tribal document
- U.S. Social Security card
- Certification of Birth Abroad, (Form FS-545 or Form DS-1350)
- Original or certified copy of a birth certificate, bearing an official seal

3.2.3 After identity verification, the individual shall complete the Fingerprint Card form, FD 258, the Fair Credit Report Act form, and be photographed and issued the appropriate access badge.

3.2.4 At this time the task order employee will be given one of the following forms, based on the security risk designation for the proposed support classification/position, to complete and return to the SOC within seven (7) business days:

- (i) **Low Risk Positions** - SF 85, Questionnaire for Non-Sensitive Positions
- (ii) **Moderate Risk Positions** - SF 85-P, Questionnaire for Public Trust Positions
- (iii) **High Risk Positions/Secret or Top Secret Security Clearances** – Standard Form

(SF) 86, Questionnaire for Sensitive Positions

3.2.5 For any task order employee whose name is provided to the Commission for security investigation at (ii) or (iii) level, who subsequently leaves the subject contract, due to Vendor or task order employee decision, within the first year, the Vendor shall reimburse the Commission for the cost of the investigation. If the task order or task order is scheduled for completion in under one year and the task order employee for whom a security investigation has been done leaves prior to the work being done, the Vendor and SOC shall agree on a pro-rated amount for reimbursement. The cost may range from approximately \$400.00 (moderate risk) to \$3,000.00 (high risk). The Vendor will be provided a copy of the investigation invoice with the reimbursement request.

3.3 Monthly Vendor Personnel Reports

The monthly report verifying task order personnel working at the FCC is a crucial element in the agency's compliance with Homeland Security Presidential Directive (HSPD) 12. Accurate and timely reporting are required as part of the ongoing access control efforts as mandated by HSPD-12 and implementing directives.

3.3.1 The Vendor's Program Manager shall submit a task order personnel list to the SOC on the first working day of each month. This report shall be identified by the task order name and FCC number, and shall list all the task order employees working at the FCC in the immediately previous month.

3.3.2 The report shall highlight or list in some way those individuals who are no longer employed by the Vendor or who are no longer working on the subject contract. As well, any additional task order personnel who have been successfully processed for work on the task order since the previous report shall also be noted.

3.3.3 The report may be delivered electronically in MS Excel format. The covering email should contain a statement of certification of accuracy and should originate with the task order Program Manager or other Vendor executive personnel. The author of the email shall be considered the signatory.

3.3.4 No later than the 15th of each month, the SOC will notify the task order Program Manager, the author of the email covering the Monthly report (if different), the COTR and the Contracting Officer if the report is a) received after the first working day of the month, or b) contains errors in the listing. The notification will identify the reason for deficit in the report.

3.3.5 The first instance of either a) or b) above shall result in a Five Hundred Dollar (\$500.00) penalty against the Vendor. The assessed penalty shall increase in Five Hundred Dollar (\$500.00) increments for each subsequent Monthly report received either late or containing errors.

3.4 Checkout Processing:

3.4.1 All task order employees no longer employed on the subject contract, or at the termination of the contract, are required to report to the SOC and complete the sign-out portion of the FCC A-600, task order Personnel Record.

3.4.2 This process verifies the access badge has been returned to the SOC by the task order personnel.

(a) If the checkout processing is not completed by the task order employee, the Vendor shall take action to ensure its accomplishment no later than thirty (30) calendar days after the employee's departure from the FCC.

(b) The Vendor shall be liable to the FCC for an administrative processing charge of \$150.00 (One Hundred Fifty Dollars), for each of their employees who leaves their duty assignment at the Commission and fails to complete the checkout processing within thirty (30) calendar days of departure. Mellon Bank, N.A., handles collection and processing of all Commission administrative charges and should payment become necessary, the Vendor will be provided the appropriate directions for an EFT.

(c) The Vendor shall be liable for any actual damages arising from a failure to ensure that the checkout processing occurs within the thirty (30) calendar days of the task order employee's departure from the FCC.

B. Drug-Free Workplace.

Within thirty (30) days of award of this task order the Vendor shall provide the COTR and CO with the documentation required under FAR 52.223-6, concerning the establishment and maintenance of a Drug-Free Workplace program. The Vendor shall further provide the COTR and CO with any materials in further support of and detailing their corporate policy in this regard.

17. ACCESSIBILITY CONSIDERATIONS

The Federal Communication Commission (FCC) considers accessibility to information a priority for all employees and external customers, including individuals with disabilities. The FCC has established Requirements for Accessible Software Design. In order to support its obligations under Sections 504 and 508 of the Rehabilitation Act of 1973, 29 U.S.C. 794 and 794d, as amended, to ensure the accessibility of its programs and activities to individuals with disabilities, specifically its obligations to acquire accessible electronic and information technology. Therefore, when selecting computer hardware and software applications for use within the FCC's computing environment, the Commission will require the Contractor to evaluate the hardware and software to determine its accessibility by users with disabilities. FCC's accessibility requirements are contained in Attachment 6.

18. GENERAL

- a. Hours of Operation.** All required activity shall be accomplished during normal working hours which are 8:30 am to 5:30 pm, Monday through Friday. Contractor staff will not be permitted to work Saturdays, Sundays or legal holidays unless authorized in writing by the CO.

- (1) Federal Holidays.** The FCC will be closed, and no contractor work authorized, for the following holidays:

New Year's Day
Inauguration Day (2009)
Martin Luther King's Birthday
President's Day
Memorial Day
Independence Day
Labor Day
Columbus Day
Veteran's Day
Thanksgiving
Christmas

When one of the above designated holidays falls on a Saturday, the preceding Friday will be observed as a legal holiday. When one of the above designated holidays falls on a Sunday, the following Monday will be observed as a legal holiday.

- (2) Inclement Weather Days.** In the event of inclement weather the Contractor is responsible for listening to the public media to determine if the FCC has been closed as a result of the weather. The Contractor is reminded that there will be no payment for any labor or services for hours the FCC is closed due to inclement weather.

- b. Supervision of Contractor Employees.** The Contractor's employees will remain under the Contractor's direct supervision at all times. Although the FCC will coordinate directions with the scope of work of the contract, detailed instructions for Contractor employees and supervision of individual workers shall remain the responsibility of the Contractor.

19. LIST OF INSTALLATION-ACCOUNTABLE PROPERTY AND SERVICES

The Contractor is authorized use of the types of property and services listed below, to the extent they are available, in the performance of this contract within the physical borders of the installation which may include buildings and space owned or directly leased by the FCC in close proximity to the installation, if so designated by the Contracting Officer.

- (a) Office space and work area space, including desks, chairs, and telephones. (Government telephones are available for official purposes only.)
- (b) The Contractor shall not bring to the installation for use under this contract any property owned or leased by the Contractor, or other property that the Contractor is accountable for under any other Government contract, without the Contracting Officer's prior written approval.
- (c) Building maintenance and utilities for facilities occupied by Contractor personnel.

20. AVAILABILITY OF FUNDS (52.232-18) (APR 1984)

Funds are not presently available for this contract. The Government's obligation under this contract is contingent upon the availability of appropriated funds from which payment for contract purposes can be made. No legal liability on the part of the Government for any payment may arise until funds are made available to the Contracting Officer for this contract and until the Contractor receives notice of such availability, to be confirmed in writing by the Contracting Officer.

21. LIST OF ATTACHMENTS

The following attachments constitute part of this task order:

<u>Attachment</u>	<u>Description</u>	<u>Date</u>	<u>No. of Pages</u>
1	Non-Disclosure Agreement	Nov. 2002	1
2	FCC FORMS:		
	a. FCC A-200, FCC Computer System Application Access Assignment Form	Jul. 2002	2
	b. FCC A-600, Contract Personnel Record	Apr. 2003	4
3	Successful Proposal		TBD
4	FCC Instruction #1479.2, Computer Security Program Directive	Oct. 2001	32

5	Contracting Officer's Technical Representative (COTR) Delegation		TBD
6	Accessibility Standards, Section 508 of The Rehabilitation Act (by reference only)		
7	FCC Policy Statement on the Prevention of Workplace Violence	Jun. 2003	1
8	FCC Instruction #1139 "Management of Non-Public Information" (to be provided to the successful offeror at time of award)	Oct. 2001	12

Quotation Cover Page

Company Name:

Name, Title, Email Address and Phone Number of Company Representative for GSA Orders:

Payment Terms:

GSA Schedule Number and expiration date:

Please check business size: () Large () Small () Minority () Women-owned

TIN:

DUNS:

NAICS:

Standard Product Code (SPC):

Complete Mailing Address:

Other Pertinent Information:

Offer Acceptance Period (no less than 60 days from due date of proposal):

Name, Title, Email Address and Phone Number of Person Authorized to Sign Offer:

Signature:

Date:

NON-DISCLOSURE AGREEMENT

I, _____, as an employee/subcontractor/consultant/representative of _____ (Contractor), operating under the terms and conditions of Contract No. _____ with the Federal Communications Commission (FCC), understand that during the course of performing duties relating to such contract or subcontract, I may be furnished or provided access to non-public information that is the property of, submitted for review or evaluation by, or collected or results from the performance of the contract between _____ (Contractor) and the FCC, and that such confidential/proprietary information shall be used only as directed.

I certify that I will not disclose any non-public information to any Contractor employees nor to any non-contractor personnel except those who have been authorized in writing by the FCC to receive such information and who have executed the same or similar Non-Disclosure Agreement. This agreement shall not be assigned, delegated nor any right or duty hereunder be transferred to any other individual or organization. I understand that the prohibition on disclosure of the protected information is an ongoing obligation and does not terminate with completion of the contract work.

CONFLICT OF INTEREST

In connection with performance of my work under or relating to this contract, I agree to abide by provisions contained in the contract's Conflict of Interest clause. I further agree that I will not will not dispute the validity of, nor take positions inconsistent with, the work product generated for the FCC in connection with this contract.

Signature

Printed Name

Date

Title

Company

Address

Witness

Printed Name

Date



FCC Computer System Application Access Assignment Form

Employees and contractors who are requesting application access must have this form completed and returned to the Application Owner. Access must be granted in accordance with FCC Instruction 1479.2 Computer Security Program Directive.

USER INFORMATION (To be completed by Application Owner)

User Name (<i>Print Last, First MI</i>):	User Name ID:
Bureau/Office or Contract Name:	Date Access Required:
Major Application Access:	Access Level:

APPLICATION RULES OF BEHAVIOR ACKNOWLEDGEMENT (To be completed by user and returned to Application Owner when Completed)

I have received a copy of the attached Application Rules of Behavior that provide information on Federal regulations, user responsibilities and the consequences of my actions, and computer security policies and procedures. I have read and will fully comply with the rules in their entirety. I recognize that it is my responsibility to ensure that I comply with the Federal computer security policies and procedures described in the FCC Computer Security Program Directive.

Printed Name: _____

Organization: _____

Signature: _____

Date: _____

ACCESS APPROVAL

I am aware that the following access has been granted to this userID:

☐ Privileged, Administrative Account.

☐ Non-Privileged, Non-Administrative User Account

Supervisor or COTR (*Printed Name*):

Signature:

Date:

Application Security Custodian (*Printed Name*):

Signature:

Date:

Return this form to the Computer Security Officer, Room 1-A325
445 12th Street, S.W., Washington, DC 20554

APPLICATION RULES OF BEHAVIOR

Passwords:

- ☐ Passwords must be at least characters long.
- ☐ Do not write down passwords.
- ☐ Do not share your passwords or accounts with others.
- ☐ Enable a password protective inactivity screensaver at your station.
- ☐ Passwords are to be changed every days.
- ☐ Use paraphrases instead of dictionary words when creating passwords.

Electronic Data/Media and Paper:

- ☐ Do not post system sensitive material in areas subject to public traffic or viewing (offices next to windows on ground floors please take special note).
- ☐ Do not transport system sensitive material in an unprotected manner.
- ☐ Lock down all sensitive unclassified material when leaving your work area.
- ☐ Protect sensitive unclassified information from alteration, disclosure or loss.
- ☐ Ensure all storage media are reformatted before they are removed for storage in a protected environment.
- ☐ Ensure that appropriate warning labels are printed on each and every page of the sensitive documentation.
- ☐ Prevent dumpster diving--do not discard system sensitive materials or communications in public trash containers.
- ☐ Deleting a file does not remove its data from the media. Use utilities which delete with overwriting before releasing media for other assignments or to ensure its destruction.
- ☐ Access only information for which you are authorized, "need to know/access."
- ☐ Respect the copyright on the material you reproduce.
- ☐ Backup data files at frequent intervals.
- ☐ Respect and protect the privacy and confidentiality of records and privacy act information while in your custody.

Dial in Access:

- ☐ Dial in users must ensure that adequate safeguards are in place on the remote computer to ensure the security of the system to which you are dialing in to.
- ☐ Lock your terminal or log off if you must leave the work area even briefly.

Laptops:

- ☐ Login IDs, passwords and /or sensitive information should not be saved on the hard drive. Use a diskette/CD to save information.
- ☐ Protect passwords and user ID's from hacker, electronic eavesdroppers or shoulder surfers.

Internet Usage:

- ☐ Do not transmit sensitive information via the internet.
- ☐ Keep your anti-virus software current.
- ☐ Periodically virus scan your client.
- ☐ Virus scan all e-mail attachments.
- ☐ Do not open executable attachments.

General:

- ☐ Use FCC computing resources when accessing applications in a manner consistent with its intended purpose.
- ☐ Report sensitive circumstances to the help desk.
- ☐ Politely challenge unescorted visitors in your area (request identification and purpose).
- ☐ Be alert to the risk of theft, espionage and intrusion in the areas you work in and take appropriate countermeasures.
- ☐ Attend or participate in annual information security training.
- ☐ Report violations of security policies or procedures that come to your attention.
- ☐ Prevent social engineering--do not reset passwords for any person via telephone until the identity of the requestor has been confirmed and verified.
- ☐ Do not divulge account access procedure to any unauthorized user.
- ☐ Users are not permitted to override technical and management controls.

FCC SECURITY OPERATIONS CENTER CONTRACT PERSONNEL RECORD

THIS SECTION TO BE COMPLETED BY CONTRACTOR'S PROJECT MANAGER

1. Risk Designation (For SOC use only)	2. Contract Personnel Name	3. Position Title
4. Secret or Top Security Clearance Required for Position? Yes _____ No _____		
5. Contractor Company Name	6. Sub-Contractor Company Name (If Any)	
7. New Contract Personnel <input type="checkbox"/> Replacement <input type="checkbox"/> Reassigned (date _____) <input type="checkbox"/>		
8. If Replacement or Reassigned, Name of Person Who Vacated the Position [Reassignment may require new A-200]		

THIS SECTION TO BE COMPLETED BY CONTRACTING OFFICER or COTR

9. New Statement of Work? Yes _____ No _____ If YES, make sure SOC has received a copy.		10. Funding Source: <input type="checkbox"/> Auctions % OR <input type="checkbox"/> Appropriated	
11. Contract/Purchase Order Number(s)		12. Task Order Number	13. Date of Award
14. Task Description (Title of Contract or Statement of Work)			
15. Description of Duties and Estimated Length of Employment:			
16. ADP/Computer Access? _____ Yes _____ No If Yes, a copy of the completed, signed FCC Form A-200 must be on file with the SOC.			
COTR Name (Print)		COTR Signature	COTR Bureau
			Phone:
			Date:
Contracting Officer Name (Print)		Contracting Officer Signature	Phone:
			Date:

THIS SECTION TO BE COMPLETED BY CONTRACT PERSONNEL

17. FCC Location: (floor and nearest room #)			
18. I understand and certify that when my work on the above-referenced contract, or any subsequent FCC contract to which I am assigned, is finished, I shall return my security badge to the Security Operations Center.			
_____		_____	
Name (Print)		Signature	
_____		_____	
Date			
In-Processing _____		Out-Processing _____	
Initials	Date	Initials	Date

OF 306 on File Yes___ No___
If No, Waiver required: SOC_____ CSO:_____

OF 306 on file: ____ Yes ____ No
If No, Waiver required:
SOC: CSO:

INSTRUCTIONS ON COMPLETING FCC Form A-600 THE FCC CONTRACT PERSONNEL RECORD

The FCC has developed this form, A-600, the FCC Contract Personnel Record, to document certain necessary risk and sensitivity information for the FCC Security Operation Center.

The FCC Form A-600 has three sections; to be completed by the Contractor's Program or Project Manager, the Contracting Officer and/or (COTR), and the Contract Personnel.

Program Manager Section:

2. **Contractor Name:** This should be as it will appear on the ID badge
3. **Position Title:** Should be exact and include levels (i.e., I, II, III, IV), if applicable.
4. **Security Clearance Required for Position:** This confirms that a Secret or Top Secret access level is required for the position duties. Most contractor positions do not require this access level.
5. **Contractor Company Name:** Must be as it appears on the contract.
6. **Sub-Contractor Name:** If any, goes here.
7. **New/Replacement/Reassigned:** Check appropriate box.
8. **Name of Replaced Contractor Personnel:** (if any)
9. **New Statement of Work?** A copy must be forwarded to the SOC.
10. **Funding Source:** Indicate percent funded by Auctions, if any.
11. **Contract/Purchase Order Number(s):**
12. **Task Order Number:**
14. **Task Description:** May be the title of the contract or statement of work.
15. **Description of Duties:** This is very important. Please be brief and to the point.
16. **ADP/Computer Access:** Contract Personnel must have completed FCC Form A-200 before they can be granted access to the FCC network. A copy of the completed A-200 must be provided to the SOC. Their level of access will depend on the details of the task.

Contractor Personnel Section:

17. **FCC Location:** The physical location, if known, of the contractor personnel.
18. **Contractor Personnel Agreement to submit to Out-Processing:** Printed name and signature that the statement has been read; to be initialed and dated at the time of In-Processing.

The SOC will complete the remaining form in order to determine final placement. SOC will confer with the COTR and/or the Contractor's Program/Project Manager for assistance in completing the FCC Contractor Position Designation Justification form.

PRIVACY ACT STATEMENT


The Federal Communications Commission (FCC or Commission) is authorized to request this information under 5 U.S.C. Sections 1302, 2951, 3301, 3372, 4118, 8347, and Executive Orders 9397, 9830, and 12107. This form is for contract personnel working for the Commission. If necessary, and usually in conjunction with another form or forms, this form may be used in conducting an investigation to determine your suitability or your ability to hold a security clearance, and it may be disclosed to authorized officials making similar, subsequent determinations.

ROUTINE USES: Any disclosure of this record or information in this record is in accordance with routine uses found in System of Records Notice OPM/GOVT-1, General Personnel Records. The Commission may disclose this information under the following circumstances:

- (1) To the appropriate Federal, State, or local agency responsible for responsible for investigating, prosecuting, enforcing, or implementing a statute, rule, regulation, or order, when the FCC becomes aware of an indication of a violation or potential violation of a civil or criminal law or regulation.
- (2) To disclose information to any source from which additional information is requested (to the extent necessary to identify the individual, inform the source of the purpose(s) of the request, and to identify the type of information requested), when necessary to obtain information relevant to an agency decision to hire or retain an employee, issue a security clearance, conduct a security or suitability investigation of an individual, classify jobs, let a contract, or issue a license, grant, or other benefits.
- (3) To disclose to a Federal agency in the executive, legislative, or judicial branch of government, in response to its request, or at the initiative of the FCC, information in connection with the hiring of an employee, the issuance of a security clearance, the conducting of a security or suitability investigation of an individual, the classifying of jobs, the letting of a contract, the issuance of a license, grant, or other benefits by the requesting agency, or the lawful statutory, administrative, or investigative purpose of the agency to the extent that the information is relevant and necessary to the requesting agency's decision.
- (4) To provide information to a Congressional office from the record of an individual in response to an inquiry from that Congressional office made at the request of the individual.
- (5) To disclose to another Federal agency, to a court, or a party in litigation before a court or in an administrative proceeding being conducted by a Federal agency, when the Government is a party to the judicial or administrative proceeding.
- (6) To the Department of Justice, or in a proceeding before a court, adjudicative body, or other administrative body before which the Commission is authorized to appear when:
 - (a) The Commission, or any component thereof; or
 - (b) Any employee of the Commission in his or her official capacity; or
 - (c) Any employee of the Commission in his or her individual capacity where the Department of Justice or the Commission has agreed to represent the employee; or
 - (d) The United States, when the Commission determines that litigation is likely to affect the FCC or any of its components, is a party to litigation, or has an interest in such litigation, and the use of such records by the Department of Justice or the FCC is deemed by the Commission to be relevant and necessary to the litigation provided, however, that in each case it has been determined that the disclosure is compatible with the purpose for which the records were collected.
- (7) By the FCC or by the Office of Personnel Management (OPM) to locate individuals for personnel research or survey response, and in the production of summary descriptive statistics and analytical studies in support of the function for which the records are collected and maintained, or for related workforce studies. When published statistics and studies do not contain individual identifiers, in some instances, the selection of elements of data included in the study may be structured in such a way as to make the data individually identifiable by inference.
- (8) To disclose, in response to a request for discovery or for appearance of a witness, information that is relevant to the subject matter involved in a pending judicial or administrative proceeding.

[The 4th page of the A-600 is left intentionally blank]

Attachment 4

 FEDERAL COMMUNICATIONS COMMISSION Washington, DC 20554 FCC DIRECTIVE	FCC DIRECTIVE	
	FCCINST 1479.2	
	Effective Date: October 2, 2001	Expiration Date: October 2006

To: All Employees and Contractors
Subject: FCC Computer Security Program

1. PURPOSE

This directive establishes policy and assigns responsibilities for assuring that there are adequate levels of protection for all FCC computer systems, Personal Computers (PCs), Local Area Networks (LAN), the FCC Network, applications and databases, and information created, stored or processed, therein. This document addresses issues relating to all aspects of computer systems security, including issues concerning day-to-day security safeguards, business continuity, system accessibility and authentication, software licensing, and administrative precautions, which can be taken by users of the FCC computer systems and those who manage them.

2. AUTHORIZATION

This directive fulfills the requirements of Office of Management and Budget (OMB) Circular A-130, Appendix III, The Computer Security Act of 1987 (Public Law 100-235), Government Information Security Reform Act (Public Law 106-398) and other applicable guidelines and laws.

3. CANCELLATION

FCCINST 1479.1, FCC Computer Security Program Directive, dated November 30, 1995.

4. APPLICABILITY

The provisions of this directive apply to all FCC employees, including telecommuters, and contractors (herein referred to as FCC users) who use a computer system or access computer generated data to conduct business on behalf of the FCC. This directive discusses safeguard measures to be taken for computer related information systems processing or containing sensitive and Commission critical data. The directive should also be used as a minimum standard for safeguarding other non-sensitive information processed or stored on FCC computer equipment.

DISTRIBUTION:
ALL EMPLOYEE

ORIGINATOR:
Computer Security
Information Technology Center
Office of Managing Director

5. POLICY

With all FCC computer systems, users shall have no expectation of privacy. As described in the required banner displayed at each login to FCC computer network, use of FCC computer systems is for FCC authorized purposes only. Appropriate administrative, audit and investigative efforts may result from inappropriate system use. All information within FCC systems is subject to access by authorized FCC personnel at any time. Individual users have no privacy interest in such information. Additional system usage allowances are discussed under Section 11 and 12 on Internet and Email use. All related systems and information shall be secured to at least the minimum level of security defined in this and other related FCC directives. FCC users must *not* process or store national security classified information on FCC computer systems, unless specifically authorized by both the Security Officer (Security Operations Center) and the Computer Security Officer (Information Technology Center).

6. RESPONSIBILITIES

6.1. *Managing Director, FCC*

FCC's Managing Director shall designate a senior official to have the primary responsibility for managing the Commission's Computer Security Program.

6.2. *Chief Information Officer (CIO), Information Technology Center (ITC)*

The Chief Information Officer shall perform the following duties:

6.2.1. Assign and direct a person responsible for managing the FCC's Computer Security Program.

6.2.2. Evaluate and approve the resolution of issues related to computer security.

6.3. *Computer Security Officer, FCC*

The Computer Security Officer is responsible for establishing, maintaining, directing, and coordinating implementation of this directive and for assisting FCC management and other FCC users with the development of procedures conforming to this and other related directives. Further, the Computer Security Officer will ensure that appropriate technical and administrative safeguards are in place, and complied with, to ensure an adequate level of security for FCC computer systems. To support this effort, the Computer Security Officer shall:

6.3.1. Develop overall Commission-wide computer security objectives and goals and act as the FCC computer security focal point;

6.3.2. Ensure that FCC users are provided effective security awareness training and direction on computer system practices;

6.3.3. Coordinate with the ITC Network Development Group staff, Application Integration Group and the Operations Group to provide oversight on the

process of conducting risk analyses and computer security reviews, the preparation of Continuity of Operations Plans (COOP) and security plans, and the processes involved in the conduct of certification and accreditation of major FCC applications;

- 6.3.4. Coordinate with Bureaus/Offices to provide oversight to conduct audits of computer-based programs to include periodic security inspections, and/or reviews of data in computer files to ensure compliance with this directive, and related Federal regulations and mandates;
- 6.3.5. Support FCC users with problems related to the security of FCC computer systems, and information stored therein;
- 6.3.6. Review incidents in which security lapses/breaches have occurred, prepare reports documenting specific events that lead up to the security breakdown(s), and recommend improvements for preventing future security lapses/breaches.
- 6.3.7. As requested by the Inspector General, assist on investigative matters, when relating to computer security;
- 6.3.8. Coordinate with Performance Evaluation and Records Management (PERM) to ensure compliance with the Freedom of Information Act (FOIA) and the Privacy Act of 1974 (PA), when requests pertain to information stored on the FCC network, or components therein;
- 6.3.9. Certify, as appropriate, that all sensitive FCC computer systems and associated security safeguards comply with this directive, Federal regulations, and related mandates prior to implementation in a production processing environment;
- 6.3.10. Manage the ITC Computer Incident Response Teams (CIRT);
- 6.3.11. Act as the Commission's focal point for computer security related advice.

6.4. *ITC, Operations Group*

The Operations Group (OG) will assist with the implementation of this directive and its policy and standards. To support this effort, OG shall:

- 6.4.1. Coordinate with the Computer Security Officer to establish and maintain procedures, which will ensure the security and integrity of respective FCC computer systems. Procedures should provide adequate safeguards for processing and storing sensitive data and limiting access to systems, therein.

- 6.4.2. Document event(s), and immediately notify the Computer Security Officer, whenever a known or possible breach of computer security occurs.
- 6.4.3. Take all reasonable steps to ensure that information processed or stored on FCC computer systems is kept secured while on the FCC network.
- 6.4.4. Ensure that all file server system management account passwords are changed at a minimum of every 90 days, or more frequently as required, and that passwords are provided only to persons with a bona fide need-to-know.
- 6.4.5. Establish written file and database server backup policies and procedures and ensure that they are followed.
- 6.4.6. Periodically review to ensure that only authorized software is installed on FCC computer system servers.

6.5. *ITC, Network Development Group*

ITC Network Development Group (NDG) will assist with the implementation of this directive and its policy and standards. To support this effort, NDG shall:

- 6.5.1. Develop and implement appropriate administrative and technical procedures to conform with this directive, and other related Federal regulations, and FCC directives and policies;
- 6.5.2. Compile and maintain a FCC computer system topology which clearly illustrates the entire network, including server locations, communication links, firewalls, and all other related network components maintained by the ITC;
- 6.5.3. Ensure that all system routers and firewall passwords are changed at a minimum of every 90 days, or more frequently as required, and that passwords are provided only to persons with a bona fide need-to-know;
- 6.5.4. Coordinate with the Computer Security Officer in the development and testing of contingency plans, and provide assistance on the conduct of network risk analyses;
- 6.5.5. Identify and recommend security solutions and safeguards for use on the FCC Network in order to avert or minimize potential security vulnerabilities;
- 6.5.6. Ensure that system audit logs and other available system management reports are accumulated and reviewed. Activities that show potential misuse should be forwarded to the Computer Security Officer for consideration.

6.5.7. Responsible for operation of ITC-managed firewalls, routers, and other network devices, and implementing security policies on firewalls and ITC-managed routers.

6.5.8. Ensure the integrity and security of ITC-managed firewalls and routers.

6.6. *ITC, Applications Integration Group*

ITC, Applications Integration Group (AIG) will assist with the implementation of this directive and its policy and standards. To support this effort, AIG shall:

6.6.1. Provide Bureaus and Offices assistance to develop application(s) and database that comply with this directive and other related federal mandates and policies.

6.6.2. Provide assistance to the Computer Security Officer to ensure that appropriate security reviews are conducted on FCC applications prior to being utilized in a production environment.

6.6.3. Ensure the security and integrity of UNIX and other production servers, databases and Internet application servers under AIG control.

6.6.4. Configure UNIX systems to meet security requirements.

6.6.5. Periodically review UNIX and other production systems to verify compliance with security requirements and fix any discrepancies.

6.7. *Bureau/Office Application Custodians/Managers*

Application Custodians/Managers are those Bureau/Office representatives who have the responsibility to manage respective sensitive and mission critical applications, databases, and/or information systems. (Note: ITC, Operations Group is considered the Application Manager for all general support systems.) Application Managers should comply with and implement the policies, standards and goals of this directive. They are also responsible for ensuring the development, administration, monitoring, and enforcement of internal controls, application security plans and continuity of operations plans, and incident reporting processes. Bureau/Office Custodians/Managers should contact the Computer Security Officer for technical support in the development and implementation of their policies, standards, and goals, as needed. To support the effort, Bureau/Office Managers shall:

6.7.1. Identify sensitive and mission critical systems, applications and databases, and files within their functional control.

6.7.2. Ensure that respective computer systems are used exclusively by authorized FCC users for the performance of official Commission business and that equipment is secured to prevent unauthorized use.

- 6.7.3. Ensure that sensitive and Privacy Act data are only released outside of the Commission, with the approval of the Performance Evaluation and Records Management (PERM), Privacy Act Officer.
- 6.7.4. Monitor user requirements to ensure that only those system access privileges are granted to perform current job responsibilities.
- 6.7.5. Ensure that respective computers systems follow the system backups policy (see Section 17.2)
- 6.7.6. Assist in the development of the Security Plan for the respective Major Application.
- 6.7.7. Work with Computer Security Officer to ensure that required level of computer security is put in place for each application, including contacting the Computer Security Officer at the appropriate points in the Systems Development Life Cycle (SDLC).
- 6.7.8. Report any security incidents to the Computer Security Officer.
- 6.7.9. Monitor respective systems for potential misuse and security threats.
- 6.7.10. Perform a review of user access privileges every 6 months.

6.8. *OMD, Performance Evaluation and Records Management*

The OMD, Performance Evaluation and Records Management (PERM) is responsible for ensuring that information safeguards mandated by the Freedom of Information Act (FOIA) and Privacy Act of 1974 (PA) are implemented and maintained across all FCC computer system platforms. To support this effort, PERM shall:

- 6.8.1. Determine the disclosure eligibility of data maintained on FCC computer systems based on FOIA and PA guidelines.

6.9. *Security Operations Center, Administrative Operations*

The Security Operations Staff/Personnel Security Office is responsible for:

- 6.9.1. Arranging background checks for FCC users in sensitive computer-related positions as required by applicable regulations;
- 6.9.2. Ensuring adequate physical security for locations containing FCC computer and communications devices used to support the FCC computer system function;
- 6.9.3. Granting badge access to key FCC and ITC spaces based on a need-to-access criterion.

6.10. *Contracting Officer*

The FCC Contracting Officer shall ensure that qualified persons are assigned as Contracting Officers Technical Representatives (COTRs) for each task involving the management, development, or modification of FCC computer systems and information, therein.

Ensure that each Statement of Work (SOW) and task order comply with this directive and other related FCC and federal mandates and that all SOWs issued on behalf of the FCC include criteria to require compliance with this directive and related FCC and federal mandates.

6.11. *Contracting Officers Technical Representative (COTRs)*

COTRs shall:

- 6.11.1. Ensure that each Statement of Work (SOW) regarding computer systems and information solicitations contain appropriate language to ensure compliance with this directive and related FCC and federal mandates.
- 6.11.2. As deemed necessary, select an on-site Contractor Representative (to fill the role of Contractor Security Representative) who shall:
 - Coordinate all computer system security procedures through the COTR.
 - Ensure compliance with FCC's computer security directive, and related Federal regulations and mandates.
 - Maintain a current list of names and telephone numbers for on-site/off-site contractors working on FCC contracts, which require access to FCC computer systems. In addition, ensure that a copy of each listing is provided to the Computer Security Officer.

6.12. *Authorized PC/LAN System Users.*

An informed, educated, and alert user is a crucial factor in ensuring the security of FCC's computer systems and sensitive information resources. To support this effort, users shall:

- 6.12.1. Be aware of, and understand responsibilities to comply with this and related FCC directives.
- 6.12.2. Recognize the accountability for all activity taking place with the assigned userID and associated account.

- 6.12.3. Use FCC computer system resources only for lawful and authorized FCC business purposes, and access FCC computer systems and information only when a bona-fide business purpose exists.
- 6.12.4. Ensure that computers *are not* used to generate or send harassing or slurring messages, or similar graphical images.
- 6.12.5. Change passwords on assigned accounts every 180 days, at a minimum.
- 6.12.6. Use a password protected Screen Saver when leaving a logged-in workstation unattended.
- 6.12.7. Comply with safeguards, policies, and procedures that prevent unintentional or deliberate access to FCC computer systems by unauthorized persons.
- 6.12.8. Comply with the terms of software licenses and only install licensed software that is authorized for use at the FCC (see 14.1. Installing Non-FCC Standard Software on FCC Computers.) In addition, *do not* install or use game software on FCC computer systems.
- 6.12.9. Ensure that appropriate forms are completed and submitted pertaining to FCC computer systems access and use of resources, including: FCC Computer System Security Acknowledgement, Form A-201 (attached), used as Rules of Behavior to verify users obligation to secure the Commission's computer system and data; FCC Computer System Personally-Owned Software Certification, Form A-202 (attached), used to identify properly licensed personal software to be installed on a particular PC; and FCC Computer System Separation Clearance, Form A-203 (attached), used to announce the user's intention to relinquish computer systems access rights.
- 6.12.10. Promptly report known or suspected unauthorized use of computer resources, disclosure of user ID's and/or passwords to persons other than the assigned individual, or violations of this directive to the Computer Security Officer.
- 6.12.11. Attend mandatory FCC Computer Security Awareness Training as announced by the Computer Security Officer.
- 6.12.12. User shall not reconfigure desktop security settings without approval from the Computer Security Officer.

7. SYSTEM ACCESS CONTROLS

- 7.1. User Identification and Authentication. User identification and authentication occurs whenever a computer session is established. To support this process, each

user must use a unique userID/password. The following standards should be followed by FCC users:

- Each user must have a unique userID to access FCC computer systems. Under normal circumstances, users should not share their userID or password with anyone. In emergency situations where the user must provide the Computer Resource Center (CRC) or their supervisor access to their account, the user should change the password immediately upon the next login.
- ITC System Administrators should review audit logs to determine if there have been repeated unsuccessful attempts to login to FCC computer systems.
- Training and maintenance userIDs should be administered through a secure and documented process. These userIDs must be rendered unusable when not being used for training or maintenance tasks.
- In general, userIDs are not permitted to initiate multiple concurrent logins to access FCC computer systems. Exceptions are considered on a case-by-case basis, as approved by the Computer Security Officer.
- If using automatic login scripts for system access, the script *must not* contain the user's login password.

7.2. Password Controls. Passwords are an accepted method of authentication at the FCC and play a vital role in securing access to any FCC computer system. Passwords should be stored with one-way encryption, where only the user has the ability to know the password. The following are standards on password use for access to FCC computer systems:

- Users should select strong passwords (i.e., not the same or reverse as the userID, not the user's name or initials, not words easily found in a dictionary, etc.).
- Users forgetting their password and requiring the password to be reset, will report to the Computer Resource Center (CRC) and show their badge for proper identification, prior to the CRC resetting their password.
- Remote users forgetting their password and requiring the password to be reset will call the CRC and provide appropriate identification (e.g. badge number, or other previously determined identification (e.g. pass phrase, special identifier, etc.)) to the CRC, prior to the CRC resetting their password.
- Use passwords with a minimum length of six characters (Using a password with a combination of alphanumeric and special characters is preferred, i.e. b4time%).

- Under all circumstances, a unique userID and password, only known by the user, must be used to access FCC computer systems.
- User should change passwords periodically, but at a minimum of every 180 days, as required by the respective system.
- Users should *not* write passwords down, but should be easily remembered.
- Users must run a password protected Screen Saver when leaving a workstation unattended.
- When a password has been, or is believed to have been compromised, a new password should be established and the user should immediately contact their supervisor or COTR and the Computer Security Officer.
- ITC System Administrators are required to set userID to be revoked if a password attempt threshold of three failed login attempts is exceeded. When the threshold is reached, account should be locked from access and scheduled to reset after 15 minutes.

7.3. Application/Data Base Controls. Controls should be implemented to ensure the integrity of FCC computer systems. These controls should make certain that information and resources correctly reflect the expected and understood configuration and composition of data, applications, and programs operating on FCC computer systems.

- FCC users should be restricted to only those application systems and data required for the efficient completion of their job responsibilities. The application custodian should perform a review of user access privileges every 6 months.
- Access control software and/or network operating system security should be kept current and controls limiting user access to sensitive data, applications, and programs should be in place.
- When technically possible, logs should be maintained to monitor system usage, and used to establish accountability for changes to data and programs.
- Ensure that software license agreements are adhered to, and as required, ensure that software-metering mechanisms are in place and used to monitor software use.
- Ensure that network applications installed on FCC system servers are designated as execute-only or read-only, as necessary.

- Updates and changes to applications/databases should be thoroughly tested, prior to the deployment in a FCC production environment, to prevent unintentional access capabilities.

8. INFORMATION SYSTEM ACCESS CONTROLS

- 8.1. Obtaining System(s) Access. The Computer Resource Center staff and the Computer Security Officer have established procedures, which, in conjunction with appropriate request forms, will allow personnel to access FCC computer system resources. Each user profile and access authorization must be supported by appropriate request forms. It is vital to the security of FCC computer systems that users only request access to data and systems for which a need-to-access exists. The FCC Computer System Security Acknowledgement, Form A-201 (attached and available on the intranet), must be properly completed and submitted to the CRC to obtain system(s) access.

FCC users can acquire forms and instructions by contacting the Computer Resource Center. The Bureau/Office Assistants for Management and/or Computer Resource Center (CRC) can also assist users in determining the type of access required and in completing forms.

- 8.2. Modifying System(s) Access. One important aspect of managing computer systems is to ensure that user privileges are kept up-to-date. At various times, a user may require modified systems access to perform position functions. As access requirements change, users must complete and submit the FCC Computer System Access Request form to the CRC for appropriate action.
- 8.3. Temporarily Suspending a Users Access. Periodically users may not require access to FCC computer systems (i.e., maternity/paternity leave, extended leave without pay, extended sick leave, etc.). In these situations, users or their supervisor, should notify their Bureau/Office Assistant for Management and the CRC to have their account temporarily suspended. This process is easily accomplished by submitting a priority electronic mail (email) message to the CRC with a courtesy copy to the Computer Security Officer. When the user returns to duty, the access can easily be reactivated by contacting the CRC. This process will ensure that unused access rights to the respective system are secured until the rightful user returns.
- 8.4. Removing System(s) Access. Prior to employment termination, each FCC user working at or for the FCC, must return and/or sever all computer access rights. To facilitate this process, Bureau/Office Assistants for Management must submit an email to the "sign out" group announcing the users intended departure. It will be the responsibility of the system administrator to update their respective systems. All files contained in the users directory(ies) will be made available to the user's supervisor once access is terminated. Options available to the supervisor/COTR include transferring files to a different user, transferring the files to diskette, or purging the files from the system, if applicable.

- 8.5. Emergency System(s) Access Termination FCC managers, COTRs, or contractor managers who must have computer access authorization revoked or terminated for FCC users in an emergency situation should immediately contact their Bureau/Office Assistants for Management and the Computer Resource Center (CRC). CRC staff will ensure that proper measures are taken to initiate the access termination process. The requestor of an emergency termination action must follow-up with appropriate documentation supporting the request.

9. AWARENESS, TRAINING, AND EDUCATION

The Computer Security Act of 1987, P.L. 100-235, was enacted to improve the security and privacy of sensitive information in Federal computer systems. As one way of meeting that goal, the law requires that "each agency shall provide for the mandatory periodic training in computer security awareness and accepted computer practices of all employees who are involved with the management, use, or operation of each federal computer system within or under the supervision of that agency."

It is FCC policy that each FCC user having access to computer resources will attend the FCC Computer Security Awareness Training Program. The program will generally include discussion on the topics of computer security basics, acceptable computer practices, and an overview of computer security policies and procedures. FCC users will be instructed on training dates, times, and location several weeks prior to the training.

- 9.1. Orientation Training. Each new user of FCC computer systems shall be provided orientation training materials which outline responsibilities on safe computer practices. In addition to the training materials provided, a user can view training videos, which will discuss common sense precautions when operating computer systems, and the user's security responsibilities.
- 9.2. Annual Training. As with Orientation Training, the objective of the annual training program is to enhance users' knowledge of good security practices while operating FCC computer systems. Training topics will include computer security policy, security planning and management, and general user practices which will maintain an acceptable overall security posture of information and associated systems. The format for different audiences will vary, but the message will be the same.
- 9.3. Security Briefings. As necessary, security briefings serve to inform specific groups of situations or up-coming events which require computer security related attention (i.e., specific Bureau/Office program needs, etc.).

10. REMOTE FCC NETWORK ACCESS

Appropriate access controls must be in place to support dial-in access to FCC computer systems. Remote interfaces to FCC computer systems will provide similar security to that available when connecting to the system locally. The following guidelines are used by FCC users and ITC System Administrators to facilitate secure dial-in/out communication with FCC computer systems:

- Dial-in ports are protected from unauthorized access.
- Controls are established to ensure that remote users are authenticated before connection to the network is authorized. Further, remote system(s) access using Guest accounts *must* be prohibited. Users must have a unique userID that meets the requirements of section 7.1 of this Directive.
- Users are granted access to only the information for which they are authorized and have a need to access.
- Dial-in to FCC computer systems only occurs through entry points approved by ITC.
- Updates and changes in system communication hardware and software are tested thoroughly to prevent unintentional access exposures.
- Reasonable care is taken to protect communication equipment and telecommunications cables from unauthorized access. Any installation or adjustment of communication equipment is coordinated with the ITC, NDG.
- Users are required to attend training, which includes proper security precautions, before receiving a remote access account.

11. INTERNET ACCESS

Internet access is provided to every FCC user as a resource to directly facilitate work. In addition, accessing the Internet will broaden FCC users understanding of the general structure and availability of resources on the worldwide system of computer networks and how these resources might be applied at the FCC. For these reasons, FCC users are encouraged to explore the wide variety of sites on the Internet. While it is the intention of the FCC to provide access to and encourage exploration of this state-of-the-art computer technology, it is also the Commission's responsibility to manage access to these systems.

- 11.1. Work Related. Internet access provided by the FCC is intended primarily for work related purposes. To the extent possible, users should become informed of an Internet site's primary information content prior to actually connecting to it. In some cases the site name will be highly revealing. It is the user's responsibility to exercise good judgment when accessing Internet sites and avoid sites that might cause embarrassment to the FCC. For example, Internet sites containing sexually explicit, oriented or related material should not knowingly be accessed using FCC computer resources.
- 11.2. Limited Personal Use. In addition to accessing web sites in order to learn about their possible applicability to the FCC, users also may make limited personal use of the Internet during non-work time. Such use must not interfere with official duties, must involve minimal impact on the government, and must be consistent with the Standards of Ethical Conduct contained in 5 CFR Part 2635 and Part 19 of the Commission's rules. See below for examples of impermissible uses.

In the past, the Commission has permitted access to the Internet whenever it could be justified as serving a work-related purpose. Consistent with recent guidance applicable to federal agencies, the Commission has determined that it is appropriate to establish a new policy under which employees may make limited personal use of the Internet on non-work time. Non-work time consists of time when users are not otherwise expected to be addressing official business, including before or after work, during lunch and breaks during the day.

- 11.3. Telecommuters. The policy of allowing limited personal use of the Internet on non-work time applies to all FCC users, including telecommuters. Consistent with the rule that employees may make limited, occasional personal use of this service, the FCC's Internet connection should not be used by telecommuters as a substitute for their own Internet service provider.
- 11.4. System Monitoring. Each FCC user is identified as a member of the FCC staff and as a member of the Federal government (i.e., John Doe FCC user ID = "jdoe@fcc.gov") when accessing the Internet. Most Internet site managers monitor or audit usage of their site and can provide lists of users to various entities. Further, all Internet connectivity via FCC computer systems is logged and recorded, is an official record, and may be monitored. Inappropriate or illegal activity discovered during routine audits will be forwarded to authorities for appropriate action.

11.5. Impermissible Personal Uses

Inappropriate personal use of computer resources includes:

- Any personal use that could cause congestion, delay, or disruption of service to any government system or equipment. For example, continuous data streams (e.g. video files) or other large file attachments can degrade the performance of the overall functionality of the FCC network and would thus be an inappropriate use.
- Using the FCC systems to launch illegal computer-based attacks or to gain unauthorized access to other systems.
- The creation, copying, transmission, or retransmission of chain letters or other unauthorized mass mailings regardless of the subject matter.
- Using the FCC system for activities that are illegal, inappropriate, or offensive to fellow employees or the public. Such activities include, but is not limited to: hate speech, or material that ridicules others on the basis of race, creed, religion, color, sex, disability, national origin, or sexual orientation.
- The creation, download, viewing, storage, copying or transmission of sexually explicit or sexually oriented materials.

- The creation, download, viewing, storage, copying or transmission of materials related to illegal gambling, illegal weapons, terrorist activities, and any other illegal activities.
- Use for commercial purposes or in support of "for-profit" activities or in support of other outside employment or business activity (e.g. consulting for pay, sales or administration of business transactions, sale of goods or services).
- Engaging in any outside fund-raising activity, endorsing any product or service, as provided in 5 CFR 2635 of the Standards of Ethical Conduct.
- Participating in any lobbying activity except as provided by law, or engaging in any prohibited partisan political activity prohibited by law.
- Use for posting agency information to external newsgroups, bulletin boards or other public forums without authority. This includes any use that could create the perception that the communication was made in one's official capacity as a federal employee, unless appropriate Agency approval has been obtained, or use is at odds with the agency's mission or positions.
- The unauthorized acquisition, use, reproduction, transmission, or distribution of any controlled information including computer software and data, that includes privacy information, copyrighted, trade marked or material with other intellectual property rights (beyond fair use), proprietary data, or export controlled software or data.

12. ELECTRONIC MAIL

The FCC Electronic Mail (email) facility offers FCC users with an efficient way to communicate with others inside, and outside (via Internet) the FCC using Commission computer systems. FCC email is provided for use to accomplish day-to-day business activities.

- 12.1. Distribution Protocol. Whenever possible, FCC users should limit the distribution of email to the smallest group possible in order to eliminate unnecessary network congestion. If an inappropriate email is brought to the attention of the Computer Security Officer, the "sender" will be directed to retract the message by either the email Postmaster or the Computer Security Officer. The Postmaster will retract inappropriate or unauthorized email if the "sender" is not available.

Important Note: An email message sent to the "Everyone", or similar group, reaches approximately 2,500 FCC employees and contractors throughout the United States. If the message is inappropriate or not authorized for distribution on the FCC network, there is a significant burden on the FCC.

- 12.2. FCC Email outside the FCC. Authorized FCC email users *are not* permitted to forward FCC email or attachments to personal accounts managed by public email or

Internet access service providers where the information might be compromised. Further, FCC users *are not* authorized to use the email system to send sensitive Commission information via the Internet where information might be intercepted.

- 12.3. Personal Use. FCC employees may make incidental personal use of email. Any incidental email usage may not interfere with official duties, must have a minimal effect on the government and must be consistent with the Standards of Ethical Conduct.
- 12.4. Appropriate Use of Electronic Mail. Appropriate use of the FCC email system includes generating and sending emails regarding:
- FCC mission and program related activities.
 - EEO, FCCRA, Union Activities and Leave Donation Requests.
 - Savings Bond, Combined Federal Campaign and Bloodmobile Drives.
 - Other FCC business related and endorsed activities.
 - Subject to the limitations contained in this email policy statement, brief occasional personal messages.
- 12.5. Inappropriate Use of Electronic Mail. The FCC email facility may not be used to direct personal messages to the Everyone Group or other large groups of users. For example, FCC GroupWise email system shall not be used to send or forward messages which may contain Birth and Retirement notices, For Sale or rent notices, Death notices of non-FCC staff, or the like, but rather should be posted on the FCC Bulletin Board System (BBS).

13. DESKTOP SECURITY

The FCC has an approved desktop configuration for workstations that is approved by the Computer Security Officer.

- It is the user's responsibility to control access to data and applications residing on assigned workstations.
- Any security controls in place on the desktop (e.g. antivirus software, screen saver passwords) must remain in place unless authorized by the Computer Security Officer.
- Access to the workstation must be controlled using FCC approved password controls. No modifications may be made to the FCC approved password controls unless authorized by the Computer Security Officer.

14. SOFTWARE MANAGEMENT

Software used and stored on FCC computers must be properly licensed. Non-licensed software is not authorized for use on FCC computers. In addition, software that may have been downloaded or purchased must be pre-authorized for installation on local computer

drive(s). In addition, users are not authorized to place software, which has been licensed for individual use, on any shared drive.

14.1. Installing Non-FCC Standard Software on FCC Computers. At times, FCC users may be required to use computer software programs, which are not readily available at the Commission. Computer resources, including system disk space, are limited agency assets. In order to maximize the use of our computer resources, the group(s) managing the system(s) must be aware of what is loaded on their respective system(s). FCC managers also have the responsibility to ensure that software loaded on Commission computer systems is properly licensed. To support this effort, users must obtain authorization prior to installing software on their local drives by completing the FCC Computer System Personally-Owned Software Certification, Form A-202 (attached) and submitting the form to the Computer Resource Center for processing. Conditions which will be considered prior to approving a request, include:

- Is the software to be installed intended to support official FCC business?
- Is the software only to be loaded on the user's local computer drive(s)?
- Has the software been scanned to ensure there are no computer viruses resident on the diskette(s)?
- Will the software encumber related FCC computer resources?

14.2. Single License Software. FCC users should ensure that single license software programs are not loaded on shared system drives (i.e., J:\, M:\, etc.) or shared with others, but rather loaded only on local computer drives, once approved. Software inappropriately loaded or loaded without proper approval on system shared drives may be purged from the system after notice has been given to the user(s).

14.3. Copying Software from FCC Computer Systems. Users of FCC computer resources are *not* authorized to copy software from the system. Most software installed on FCC computer systems is designated as execute-only or read-only, as necessary. Users requiring a copy of the software loaded on FCC computer systems for a remote PC should contact the Computer Resource Center for assistance.

14.4. Upgrading Software. As necessary, software will be upgraded to a newer or up-to-date version, provided funding is available. When previous versions of software are no longer installed on FCC computer systems or individual PCs, appropriate actions should be taken to ensure destruction of the old version, ensuring the software is no longer useable.

14.5. Games. Users of FCC computer resources are *not* authorized to load games software on FCC provided computer systems.

15. COMPUTER VIRUS PREVENTION AND MANAGEMENT

A virus is a piece of computer programming code usually disguised as something else that causes some unexpected and, for the victim, often an undesirable outcome. Some viruses are programmed so that they automatically spread to other computer users. Viruses can be transmitted as attachments to an email, downloaded from Internet sites, or copied from diskettes or CD. The source of the email, downloaded file, or other source of the infected file is often unaware of the virus. Some viruses wreak their effect as soon as their code is executed; other viruses lie dormant until circumstances cause their code to be executed by the computer. Some viruses are playful in intent and effect (e.g., "Happy Birthday!"). Others can be quite harmful, erasing data causing email systems to overload, and/or causing severe network outages.

The best protection against a virus is to know the origin of each program or file loaded into the computer or opened from the email program. In addition all FCC computers are supplied with antivirus software that can screen email attachments and also check all of a user's files periodically and remove any viruses that are found. From time to time, users may receive an email message warning of a new virus. Unless the warning is from the FCC Computer Security Officer, or a recognized source, chances are good that the warning is a virus hoax. It is suggested that FCC users forward any warning received from non-FCC sources to the FCC Computer Security Officer for validation.

FCC computer system users can minimize exposure to viruses by following these safe-computing practices (additional guidance is available by contacting either the CRC or the Computer Security Officer):

- Place write-protection on original software diskettes.
- Do not use unauthorized software.
- Never download programs from the Internet to the office PCs without scanning the file to be downloaded.
- Do not use shareware and demonstration software from unauthorized sources or unfamiliar vendors.
- Use an up-to-date, FCC approved antivirus program. ITC, Operations Group will ensure that the most current version of the software selected for use at the Commission is available for use. Users should scan computer drives and check diskettes prior to use, including those received from other FCC Users, or outside sources. If a virus is detected, the user should notify the CRC immediately.
- FCC users should extend the layer of virus protection to home computers by installing antivirus software on home computers. If there is not an up-to-date antivirus program on a home computer, the FCC has antivirus CDs available for home use. Apply similar antivirus precautions on the home computer as described, herein.

- Be suspicious of email attachments. Always scan executable email attachments before opening. Many infected files transmit themselves through email programs. Just because the person sending the file is known does not mean it is virus free.
- Check to ensure that Microsoft Office Applications have macro protection enabled. Once this is done, if a file is opened with a macro virus it will prompt to Enable or Disable macros. Always choose *Disable Macros* or *Do Not Open* if a Macro Dialog Protection Warning is received for a document not expected to contain macros.
- Reboot PCs at least once a day to ensure that the latest antivirus definitions are received.

16. PHYSICAL SECURITY AND COMPUTER EQUIPMENT HANDLING

The offices and work areas where FCC computer systems are located must be physically secured when unattended. Adequate controls should be employed consistent with the value, exposure and sensitivity of the information and equipment that is to be protected. Although the value of a computer can be significant, the value or importance of the information can be far greater. It is recommended that management establish controls that include any or all of the following:

- 16.1. Area Access Controls. FCC users have a responsibility to create and maintain a secure work environment, and to protect the computer assets used to fulfill business activities. Access to offices and work areas, where FCC information, and computer resources are located, should be controlled in a manner that permits access only to authorized persons. In addition, system-provided mandatory *Screen Saver* and associated password are imposed for each user of FCC PCs. The use of the *Screen Saver* with password will ensure that while the PC is unattended, no one but the person knowing the password can gain access to the system via the user's account.
- 16.2. Preventing Hardware Theft. Information and computer equipment must be protected against theft. Loss of certain information, if not properly backed-up, can require significant effort to recreate. Significant repercussions may ensue if the lost information is subject to FOIA compliance or has a business or economic impact. It is recommended that Bureaus/Offices select and implement security controls that employ any or all of the following measures:
 - *Do not* store critical or sensitive data, files, or programs on any PC's local drive. Rather, store such information on the local file server (e.g. N\ Drive). As deemed necessary by each user, periodically backup any files stored on the local computer's drive to diskette and store in a safe and secure location.
 - Only authorized FCC users should have access to areas where computer resources, processing sensitive or mission critical FCC information, are housed. Authorization to controlled areas should be granted, and removed when applicable, on a "need-to-access basis."

- Work and storage areas housing computer resources should have locked doors, cabinets, or desks in use. When computer hardware storing sensitive or mission critical information is not secured by a locked door, it should be secured with equipment enclosures and/or lock-down devices. Accessory equipment like modems and external disk drives should be secured in a similar fashion.
- Business sensitive correspondence, other printed information and magnetic media should be stored in locked containers, desks or file cabinets;
- FCC users should provide visual coverage of computer resources during business hours if the resources are not in a lockable area.

16.3. Portable Computer Resources. Portable computer resources (e.g., Laptop, Notebook, Personal Digital Assistant, etc.) provide convenience and productivity gains. However, with portable computer resources there are increased risks of theft and loss of information.

Hardware and software techniques should be employed to keep FCC information protected from unauthorized individuals in the event the portable equipment is lost or stolen. Options include, but are not limited to, lock-down devices and PC-boot passwords.

- FCC users should be particularly security conscious when traveling with portable computer resources.
- FCC users should not check FCC assigned laptop computer as baggage when traveling with commercial carriers, rather maintain possession of the laptop at all times.

Security and inventory play a key role in the management of portable computer resources. All portable resources should be kept secured in a locked storage area while stocked. Staff responsible for the management of inventory should maintain records to include, as a minimum:

- a master inventory list of all portable equipment assigned
- user's name checking out the resource
- equipment brand name
- equipment serial, bar code, and FCC numbers
- fax modem card number
- a copy of the FCC Property Pass slip

16.4. Removable Information Media. Removable media (e.g., tapes, CD-ROM, CD-R, Zip disks, floppy diskettes, etc.) allow for the storage of large concentrations of

sensitive data vital to the FCC mission. Depending on the potential exposure of information residing on removable media, managers should establish any or all of the following controls:

- Ensure that FCC users understand the significance of sensitive information contained on removable media. Additionally, advise FCC users of their responsibility to protect information on removable media as protection of this information would be required in other formats.
- Discard hard-copy information in a secure manner that prohibits the information from being retrieved and made use of by unauthorized persons.
- Develop procedures to ensure that sensitive information is not stored on diskettes unless the diskettes are properly labeled and stored in a lockable unit in an access-controlled environment.
- Encourage the use of document password controls available with FCC provided desktop applications.

16.5. Relocating Computer Hardware. PCs and related hardware are often moved from one location to another. It is important that secure methods are employed to safeguard this equipment and the information it may contain during relocation. FCC users should submit a Move Questionnaire to the building management center, requesting the relocation of computer hardware, which is then forwarded to the Operations Group (OG). OG completes the move and maintains the validity of the equipment inventory. Each Bureau/Office may consider an internal process to ensure clearance through the Assistant for Management before releasing the move request to OG.

16.6. Environmental Protection. PCs are sensitive to the quality of electrical power. As a result, surge protectors should be used to regulate electrical current and absorb abnormal electrical levels. Drinking and eating should be discouraged in the immediate vicinity of PCs and related peripherals.

The Computer Room and hub rooms contain, in most cases, the highest concentration of support equipment and information used at the FCC. Sufficient suppression systems are installed to mitigate the possibility of power spikes for incoming power supplies. In addition, surge protectors should be used on all FCC issued computers. Battery backup via an uninterruptible power supply (UPS) must be installed to provide system server(s) and peripherals support in the event of a power failure.

16.7. Telecommuting. All FCC owned computers and other equipment relocated to an employee's home for telecommuting purposes are covered by this directive. Hardware and software techniques should be employed to keep FCC information protected from unauthorized individuals. Also, passwords should be safeguarded to prevent access by unauthorized individuals to the FCC network.

17. COMPUTER SYSTEM BUSINESS RECOVERY

- 17.1. PC Data Backups. Users are instructed not to store sensitive or mission critical data on their PCs hard-drive. Users are instructed to store all sensitive and mission-critical data on the network server. However, any data that is stored on the PC's hard-drive should be protected from inadvertent loss. As a precautionary measure, users are encouraged to backup data to diskette at an interval commensurate with how often data changes are made, and secure the diskette(s) in a safe location.
- 17.2. Application and Data Backups. To be usable, copies of electronic media must be made accurately, regularly, and consistently. ITC Operations Group ensures that adequate network backups are maintained, including files created using the standard office automation software suite. Precautions should be made to ensure that the type of media used does not become faulty over time using a periodic test scenario. Bureau/Office application managers shall ensure that adequate backups are made of bureau/office applications/databases, and data within their control.

In all cases, System Managers will use the 'son, father, and grandfather' system, the following should be considered as minimum standards in the backup process:

- Incremental (or differential) backups (data files that have been modified) should be taken daily.
- System backups (all data files) should be taken weekly.
- Application configuration backups should be taken monthly.

The means by which electronic backups are stored is as important as the backup process. The most recent backups, incremental and system, should be stored on-site for immediate access, as needed. These backup tapes must be stored in a safe location capable of protecting electronic media from environmental (e.g., fire, water, smoke, etc) concerns. After the new version of the backups are completed, the previous version must be stored off-site (ie., a different location than that of the system and current backups.) As the series of backups are made, the oldest version stored off-site should be returned to the operations site for reuse.

The current retention policy for system and data backups is to hold twelve weeks of data in the backup program (one week in the on-site safe, ten weeks at the off-site storage facility, with the final week processed back to the FCC from the off-site storage facility). The off-site location should provide similar protection against environmental threats and physical access, as that of the Computer Room. A similar backup process should be considered for independent computer systems.

- 17.3. Computer Incident Response Team. The FCC's Computer Incident Response Team (CIRT) has been charged to act as the Commission's focal point for

mitigating the impact of computer related incidents. The team is comprised of technical experts in the fields of PCs, computer networks, telecommunications, application(s) management, and security. As required, the team acts to prevent or minimize the impact of a threat against computer operations at the FCC (e.g., isolating a computer virus infection and eradicating its infection without the destruction of data, implementing the teams mitigation plan to prevent intruders from accessing FCC computer systems, taking preliminary steps to minimize the need for the agency's COOP, etc).

- 17.4. Continuity of Operations Plan. Although some risks can be minimized, they cannot be eliminated. Undesirable events occur regardless of the effectiveness of a security/control program. The Continuity of Operations Plan (COOP) provides a controlled response that minimizes damage and restores operations as quickly as possible. The COOP consists of a document that provides a course of action to be followed before, during, and after the occurrence of an undesirable event that disrupts or interrupts network operations. ITC is responsible to develop and periodically test the FCC COOP. Bureau/Office representatives involved in the implementation of the COOP will be briefed in advance and will receive a copy of the plan. The COOP will be updated annually to reflect changes in the FCC's architecture and mission priorities.

18. PERSONNEL SECURITY

As mandated by Executive Order 12968, Executive Order 10450 and OPM, 5CFR731, the FCC must conduct personnel security and suitability investigations. Each FCC User will be classified as a High, Moderate or Low Risk according to level of access to the respective systems. Background investigations will be conducted to ensure compliance with Federal Mandates.

19. SENSITIVE DATA/APPLICATION MANAGEMENT

Oversight for computer data and associated resources resides with the Bureau/Office requesting the purchase of the peripheral(s) or development of the application and/or data. Bureau Chiefs and Office Directors should assign ownership to an appropriate Division, Branch, or any functional entity within that Bureau/Office. Management responsibilities should not be construed as replacing or diluting the Computer Security Officer's or ITC CIO's responsibilities for compliance with computer security requirements.

Designated Bureau/Office Managers of FCC's computer system/applications should:

- Acknowledge responsibility of resources and identify those applications containing or processing sensitive data.
- Coordinate with the Computer Security Officer to develop protection controls.
- Authorize access to computer resources under their control.
- Educate managers and users on control and protection requirements for computer systems and information.

- Monitor compliance with established security FCC directives, Federal regulations and other applicable mandates, and periodically review control processes.

20. SENSITIVE/MISSION CRITICAL DATA

As mandated in the Computer Security Act of 1987, the FCC must determine the classification of sensitive data in its possession. Each FCC Bureau/Office owning or acting as custodian of computer based application is responsible for determining the sensitivity of those documents. The Bureau/Office representative making such decisions must consult PERM for concurrence.

Based on the National Institute of Standards and Technology (NIST) guidelines, the following criteria to determine the sensitivity and/or related mission critical nature of applications and data processed at the FCC applies:

- Information protected under the Privacy Act of 1974 and the Freedom of Information Act.
- Data and information, which is critical to an agency's ability to perform its mission.
- Financial Management Data on systems that process electronic funds transfers, control inventory, issue checks, control accounts receivable and payable, etc.
- Each Bureau/Office shall ensure that all computer-processed data created be identified. ITC must be notified, via memorandum, of all sensitive and mission critical data generated or processed by a Bureau/Office computer based application. Ad-hoc output reports shall be safeguarded in a manner commensurate with the standards established in this and the following sections.

21. SAFEGUARDING SENSITIVE/MISSION CRITICAL DATA

Each FCC Bureau/Office shall be responsible for ensuring that all forms of media (e.g., paper, diskette, CD-ROMs, cartridge, etc.) containing sensitive data originated or processed by the Bureau/Office is handled and disposed of in a manner commensurate with the criteria established in this and other FCC directives (20.1 Storing Sensitive Data). FCC users should ensure that sensitive data is not stored on shared drives (i.e., J:\ drive) where many users may have uncontrolled access to the data. In addition, users should *not* store sensitive data on their local drive (i.e., C:\). Bureaus/Offices and users requiring a secure method for sharing sensitive information should consider the use of the Novell Netware Filer utility. If properly configured, Filer safely allows multiple users to share documents in a common area (i.e., J: drive). By establishing a sub-directory using Filer, access can be controlled, allowing the custodian to define who has access to the sub-directory. The CRC can assist in setting up such sub-directories.

- 21.1. Sharing Sensitive and Other Data with Others Outside the FCC. It is the policy of the FCC that Sensitive Information (Non-Public—For Internal Use Only, Non-Public—Highly Sensitive/Restricted, financial and other types of data) only releasable by authorized Bureaus/Offices within the FCC. Further, users should

take precautions to protect the release of magnetic media containing sensitive information and should contact their supervisor for guidance, as needed.

22. DESTRUCTION OF SENSITIVE DATA

The useful life of every computer document should end with its destruction in a safe and secure manner. All forms of media (hard-copy, magnetic, etc.) containing sensitive data require a safeguarded means of destruction. The following procedures, or other processes supporting similar security procedures, should be considered within each Bureau/Office for the disposal of such reports:

- Sensitive documents should not be hoarded, but destroyed as soon as they are no longer required.
- Electronic media (diskettes, magnetic tapes, CD-ROMs, etc.) should be destroyed, or over-written.
- Material that is no longer needed and may lawfully be destroyed must be disposed of in a locked document disposal bin (in the Portals building) or other comparable method (in non-headquarters locations.)

23. IDENTIFYING SENSITIVE/MISSION CRITICAL APPLICATIONS

The term sensitive application, as defined by OMB Circular A-130, means "an application of information technology that requires protection because it processes sensitive data, or because of the risk or magnitude of loss or harm that could result from improper operation or deliberate manipulation of the application." As such, Bureaus/Offices are required to determine and notify ITC of which, if any, applications/databases controlled or utilized within that Bureau/Office are considered sensitive or support a function considered critical to the successful operation of the FCC. The information provided will become a crucial component of the Commission's COOP.

24. SENSITIVE/MISSION CRITICAL AND MAJOR APPLICATION – CERTIFICATION AND ACCREDITATION

At various times, computer applications will be created and utilized at the FCC, which process sensitive data. Prior to implementation, these applications shall undergo testing to verify that the required administrative and technical safeguards are operationally adequate and the results of the design review and system tests are fully documented and maintained. ITC in concert with the Bureau/Office managing the design of a new application/database which is intended to process sensitive data should select and assign qualified personnel to test the security of the application. Should an application require significant expansion or revision, the series of tests should re-occur. The Computer Security Officer can provide technical oversight support during all phases, as requested by the Bureau.

The personnel assigned the responsibility for system testing shall:

- Establish objectives and specifications required for security of the application.

- Define the security requirements to be included in the design of the application.
- Ensure that all security requirements included in the design phase are incorporated during the programming phases of the application.
- Consider results of the most recent network risk analysis during the application development planning phase to ensure that adequate safeguards are considered.
- Test the security of the application as it interacts with existing operational security controls on the system, and evaluate unexpected or fraudulent inputs to determine the performance of the application during unusual circumstances.
- Ensure the conduct of risk analysis for the application, as required by applicable Federal regulations.

25. SENSITIVE/MISSION CRITICAL SYSTEM CERTIFICATION

Sensitive system certification is intended to provide assurance that sensitive applications meet security related Federal regulations, as required by OMB Circular A-130, Appendix III. The certification process agreed to by the Bureau/Office Manager and the Computer Security Officer, will ensure security safeguards installed during the certification will remain in effect. Each Bureau/Office Manager and the Computer Security Officer should coordinate to complete the certification process for existing/new applications not yet certified. Re-certification of sensitive applications will occur whenever an application is modified significantly or every three years.

26. EXTERNAL COMPUTER RESOURCE SERVICES

FCC computer security directives and policies have no exclusionary provisions, but are applicable to computer systems and information/applications containing FCC information for which the FCC is the legal custodian. The boundaries of responsibility apply whether the processing services are performed at an FCC facility, by another Government agency, or by a non-government agency (i.e., contractor.)

- 26.1. Sensitive FCC Data Processed by another Government Agency. All Government agencies are required to adhere to the information security policies in OMB Circular A-130 unless more stringent policies or regulations apply at the agency where the information is being processed. Regardless of the approach, all Government agencies must adhere to the policy that sensitive applications will only be processed on computer systems having appropriate security protection, after sensitive applications have been certified to handle sensitive data by the Bureau/Office Manager and the Computer Security Officer.

- 26.1.1. It is the responsibility of the COTR, with the assistance of ITC, PERM, to determine the level of sensitivity of the data to be processed by the external organization. The computer security requirements will be made

known to the external organization during contract negotiations and prior to any contract initiation.

26.1.2. Sensitive information will be processed only on systems having appropriate security protection and which have been certified to handle such information. If the computer system is not under the control of the FCC, the certification document will be requested from the custodian/owner of the system.

26.1.3. Copies of the certification documents, provided by the outside organization, and any relevant correspondence should be maintained by the COTR.

26.1.4. Re-certification of sensitive systems or applications must be accomplished by the external organization, within the time frames set-forth in applicable Federal regulations. The data processing agreement with the organization should state that the re-certification will be accomplished as required, and that a copy of the certificate will be provided to the Computer Security Officer.

26.2. Sensitive FCC Data Processed by a Non-Government Agency. More and more Government work is being performed by non-Government agencies (i.e., contractors.) When these organizations are under contract with the FCC, the contract must specify adherence to the FCC Computer Security Program Directives. In addition:

26.2.1. Before entering into an agreement to process or handle sensitive information at a contractor facility, a security assessment of the facility should be conducted, or should have been completed within the previous three years, and the results of the analysis will be made available to the Contracting Officer for review. The Contracting Officer should consult the Computer Security Officer for technical assistance, as required.

26.2.2. The contract should specify that FCC reserves the right to perform unannounced on-site inspections of the site where FCC information is being processed. The inspections are used as a tool to ensure adherence to FCC's computer security directive and policies, and other applicable Federal regulations and mandates.

26.2.3. The COTR will monitor contractor compliance with FCC's Computer Security Program Directive and policies, therein.

27. COMPUTER SYSTEM(S) SECURITY AUDITS

At periodic intervals, it is necessary that audits be performed on FCC computer systems and applications. The primary focus for security audits of computer systems is to ensure that unauthorized or illegal activities are detected and remedied as quickly as possible. Secondary benefits to system audits support the organization's administration and management function.

For instance, routine audits of computer systems will ensure that only authorized users have access to the system/information; appropriate levels of access have been authorized and are maintained; and that previously authorized users of a system no longer requiring access are purged.

28. INCIDENT AND VIOLATION REPORTING

When a breach of computer systems security occurs (i.e., unauthorized disclosure, alteration, destruction, loss or compromise of sensitive data, resources and unauthorized access, or misuse of computer resources), incident and violation reporting serves as a means of resolution. It is imperative that any security breach be isolated and contained allowing appropriate personnel to respond to the situation. FCC users are responsible, as described in *Responsibilities* section of this directive, for promptly reporting computer system security related incidents to the Computer Security Officer.

The Computer Security Officer will coordinate with respective ITC managers, the Inspector General, and the Bureau/Office to inquire into reported information and computer security violations and collect, develop, and retain sufficient information to bring the reported computer security violation to closure.



Andrew S. Fishel
Managing Director

- FCC Computer System Security Acknowledgement, Form A-201
- FCC Computer System Personally-Owned Software Certification, Form A-202
- FCC Computer System Separation Clearance, Form A-203
- Definitions
- References

Stocked By:
Performance Evaluation and Records Management

DEFINITIONS

- a. Access - 1. The ability to enter a secured area. 2. A specific type of information between a subject and an object that results in the flow of information from one to the other.
- b. Access Control - An entire set of procedures performed by hardware, software, and administrators to monitor access, identify users requesting access, record access attempts, and grant or deny access based on pre-established rules.
- c. Adequate security - security commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information. This includes assuring that systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability, through the use of cost-effective management, personnel, operational, and technical controls.
- d. Alphanumeric - A contraction of *alphabetic* and *numeric*, that indicates a combination of *any* letters, numbers, and special characters.
- e. Application - means the use of information resources (information and information technology) to satisfy a specific set of user requirements.
- f. Availability - That aspect of security that deals with the timely delivery of information and services to the user.
- g. Backup - Applies to data, equipment or procedures that are available for use in the event of failure or loss of normally used data, equipment or procedures. The provision of adequate backup capability and facilities is important to the design of data processing systems in the event of a system failure that may potentially bring the operations of the business to a virtual standstill.
- h. Computer Log-in - A simple procedure occurring at the beginning of a session at a workstation in which the host asks the user for identification. At the FCC, login refers to two separate authorization codes: userID, and password.
 - 1. UserID is the authorization code used to verify that FCC users are entitled access to FCC computer resources, and to identify the specific resource(s) used; and
 - 2. Password is a unique secret word selected by each user that is associated with a particular user ID. The Passwords primary function is to protect the userID from unauthorized use. A non-display mode is used when the password is entered to prevent disclosure to others.
- i. Computer Security - Technological and managerial procedures applied to computer systems to ensure the availability, integrity, and confidentiality of information managed by the computer system.

- j. Data Integrity - A measure of data quality. Integrity is high when undetected errors in a database are few. Complete data integrity is the assurance that is input to the computer today will be there tomorrow, unchanged in any way.
- k. Bureau/Office Manager - Any FCC Bureau/Office representative who acts as the application/database or system focal point for management.
- l. General Support Systems - Are those interconnected set of information resources under the same direct management control which share common functionality. A system can be, for example, a local area network or an agency-wide backbone.
- m. Hardcopy - Medium of data, either input or output, in paper form such as printouts, reports, screen prints, memoranda, checks, etc. generated as a result of the use of FCC computer system resources.
- n. Major Application - An application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Note: All Federal applications require some level of protection. Certain applications, because of the information in them, however, require special management oversight and should be treated as major. Adequate security for other applications should be provided by security of the systems in which they operate.
- o. Mission Critical Data - Is any electronic data which supports the collection, transfer, or disbursement of funds, or Commission activities mandated by statute or treaty, the interruption of which would cause significant economic or social harm to licensees or the public.
- p. Removable Media - An information storage medium that can be removed from an information creation device such as a computer. Examples are diskettes, tapes, cartridges, optical disks, and external disk drives.
- q. Sensitive Information - Is that which requires various degrees of protection due to the risk and magnitude of loss or harm, which could result from accidental or deliberate disclosure, alteration, or destruction. This data includes records protected from disclosure by the Privacy Act, as well as information that may be withheld under the Freedom of Information Act, Non-Public—Highly Sensitive/Restricted and/or Non-Public—For Internal Use Only. Computer "hard copy" is considered, for purposes of this directive, a computerized record, and may contain "sensitive" data.

REFERENCES

- a. Public Law 99-474, Subject: "Computer Fraud and Abuse Act of 1986." The act provides for unlimited fines and imprisonment of up to 20 years if a person "intentionally accesses a computer without authorization or exceeds authorized access and, by means of such conduct, obtains information that has been determined...to require protection against unauthorized disclosure...." It is also an offense if a person intentionally accesses "a Federal interest computer without authorization and, by means of one or more instances of such conduct alters, damages, or destroys information...or prevents authorized use of such computer...or traffics any password or similar information...if such computer is used by or for the Government or the United States."
- b. Public Law 100-235, Subject: "Computer Security Act of 1987." The Act provides for a computer standards program within the National Institute of Standards and Technology (NIST), to provide for Government-wide computer security, and to provide for the training in security matters of persons who are involved in the management, operation, and use of Federal computer systems, and for other purposes.
- c. OMB Circular No. A-123, Revised, Subject: "Internal Control Systems." Requires heads of government agencies establish and maintain effective systems of internal control within their agencies that, in part, safeguard its assets against waste, loss, unauthorized use, and misappropriation. Among other things, the circular specifies that periodic security reviews be conducted to determine if resources are being misused.
- d. OMB Circular No. A-127, Subject: "Financial Management Systems." This Circular prescribes policies and procedures to be followed by executive departments and agencies in developing, operating, evaluating, and reporting on financial management systems.
- e. OMB Circular No. A-130 "Management of Federal Information Resources," Appendix III "Security of Federal Automated Information Resources." Requires federal agencies to implement a computer security program and develop physical, administrative, and technical controls to safeguard personal, proprietary, and other sensitive data in automated data systems. OMB Circular A-130 also requires that periodic audits and reviews be conducted to certify or recertify the adequacy of these safeguards. In addition, it makes agency heads responsible for limiting the collection of individually identifiable information and proprietary information to that which is legally authorized and necessary for the proper performance of agency functions, and to develop procedures to periodically review the agency's information resources to ensure conformity.
- f. 5 CFR Part 2635.11-12, "Standards of Ethical Conduct for Employees of the Executive Branch." Use of Government Property - Personnel shall protect and conserve Government property, including equipment, supplies and other property entrusted to them. Use of Government Information - Personnel shall not use, or allow use of, official information obtained through performance of duties to further a private interest if such information is not available to the general public.

- g. 5 USC 552, Freedom of Information Act (FOIA) of 1974, As Amended. FOIA requires agencies to make available, on its own initiative, certain types of records and disclose any other record to a requestor unless a specific exemption under FOIA, of which there are nine, applies.
- h. 5 USC 552a, Privacy Act of 1974, As Amended. The basic provisions of the act are to protect the privacy of individuals. An agency is prohibited from disclosing personal information contained in a system of records to anyone or another agency unless the individual (about whom the information pertains) makes a written request or gives prior written consent for third party disclosure (to another individual or agency).
- i. 40 United States Code 1452, Clinger-Cohen Act of 1996. This Act links security to agency capital planning and budget processes, establishes agency Chief Information Officers, and re-codifies the Computer Security Act of 1987.
- j. NIST Special Publication 800-18, Guide for Developing Security Plans for Information Technology Systems. This publication details the specific controls that should be documented in a security plan.
- k. Paperwork Reduction Act of 1995. This Act linked security to agency capital planning and budget processes, established agency Chief Information Officers, and re-codified the Computer Security Act of 1987.
- l. Federal Information Processing Standards (FIPS) Pub. 102, Guideline for Computer Security Certification and Accreditation. This guideline describes how to establish and how to carry out a certification and accreditation program for computer security.
- m. GAO/AIMD-12.19.6, Federal Information System Controls Audit Manual (FISCAM). The FISCAM methodology provides guidance to auditors in evaluating internal controls over the confidentiality, integrity, and availability of data maintained in computer-based information systems.
- n. P.L.106-398, The FY 2001 Defense Authorization Act including Title X, subtitle G, "Government Information Security Reform Act." The Act primarily addresses the program management and evaluation aspects of security. It provides a comprehensive framework for establishing and ensuring the effectiveness of controls over information resources that support federal operations.
- o. National Information Assurance Certification and Accreditation Process (NIACAP). This process (NSTISSI 1000) establishes a standard national process, set of activities, general tasks, and a management structure to certify and accredit systems that will maintain the Information Assurance (IA) and security posture of a system or site.
- p. Presidential Decision Directive 63, "Protecting America's Critical Infrastructures." This directive specifies agency responsibilities for protecting the nation's infrastructure; assessing vulnerabilities of public and private sectors; and eliminating vulnerabilities.

FCC Policy Statement on the Prevention of Workplace Violence

The Federal Communications Commission's policy is to maintain a safe work environment that is free from any form of violence. The FCC is committed to working with employees and the National Treasury Employees Union to promote a work environment free from violence, threats, harassment, intimidation, and other inappropriate behavior. FCC policy prohibits violence, threats, harassment, intimidation or other inappropriate behavior that causes fear for personal safety.

While workplace violence is not pervasive at the FCC, no organization is immune. Incidents can arise from non-work related situations, such as domestic violence, that move into the workplace. Disputes involving employees, supervisors, contractors, visitors, or members of the public can also be sources of potential violence.

Violence, threats, harassment, intimidation, and other inappropriate behavior in our workplace will not be tolerated. Such behavior can include oral or written statements, gestures, or expressions that communicate a direct or indirect threat of physical harm. All reports of incidents will be taken seriously and will be dealt with in an appropriate manner. Individuals who commit such acts may be removed from the premises and may be subject to disciplinary action, criminal penalties, or both.

All employees are encouraged to promote a safe working environment. Do not ignore violent, threatening, harassing, intimidating or other inappropriate behavior that causes fear for personal safety. If you observe or experience such behavior by anyone, employee or otherwise, report it to a supervisor in your chain of command or the Security Office immediately. Supervisors and managers who receive such reports must contact the Security Office immediately. Depending on the nature of the report, the Security Office may contact other FCC offices or the Federal Protective Service regarding investigating the incident and initiating appropriate action.

In an emergency or other threatening situation at the Portals, contact the Security Office at 418-7884, the Federal Protective Service at 202-708-1111, or dial 911. At all other locations, contact local authorities at 911.